



Privacy Advisory Commission

May 5, 2022 5:00 PM

Teleconference

Meeting Agenda

Commission Members: *District 1 Representative: Reem Suleiman, District 2 Representative: Chloe Brown, District 3 Representative: Brian Hofer, Chair, District 4 Representative: Lou Katz, Vice Chair District 5 Representative: Omar De La Cruz, District 6 Representative: Gina Tomlinson, District 7 Representative: Robert Oliver, Council At-Large Representative: Henry Gage III Mayoral Representative: Jessica Leavitt*

Pursuant to California Government Code section 54953(e), Oakland Privacy Advisory Commission Board Members/Commissioners, as well as City staff, will participate via phone/video conference, and no physical teleconference locations are required.

TO OBSERVE:

Please click the link below to join the webinar:

<https://us02web.zoom.us/j/85817209915>

Or iPhone one-tap:

US: +16699009128, 85817209915# or +13462487799, 85817209915#

Or Telephone:

Dial (for higher quality, dial a number based on your current location):

US: +1 669 900 9128 or +1 346 248 7799 or +1 253 215 8782 or +1 646 558 8656

Webinar ID: 858 1720 9915

International numbers available: <https://us02web.zoom.us/j/85817209915>

TO COMMENT:

1) To comment by Zoom video conference, you will be prompted to use the “Raise Your Hand” button to request to speak when Public Comment is being taken on the eligible Agenda item. You will then be unmuted, during your turn, and allowed to make public comments. After the allotted time, you will then be re-muted.

2) To comment by phone, you will be prompted to “Raise Your Hand” by pressing “* 9” to request to speak when Public Comment is being taken on the eligible Agenda Item. You will then be unmuted, during your turn, and allowed to make public comments. After the allotted time, you will then be re-muted.

ADDITIONAL INSTRUCTIONS:

1) Instructions on how to join a meeting by video conference is available at: <https://support.zoom.us/hc/en-us/articles/201362193%20-%20Joining-a-Meeting#>

2) Instructions on how to join a meeting by phone are available at: <https://support.zoom.us/hc/en-us/articles/201362663%20Joining-a-meeting-by-phone>

3) Instructions on how to “Raise Your Hand” is available at: <https://support.zoom.us/hc/en-us/articles/205566129-Raising-your-hand-In-a-webinar>

1. Call to Order, determination of quorum
2. Adopt a Renewal Resolution regarding AB 361 establishing certain findings justifying the ongoing need for virtual meetings
3. Review and approval of the draft April meeting minutes
4. Open Forum/Public Comment
5. Federal Task Force Ordinance – OPD – Presentation of Annual Reports (ATF, USMS, DEA, FBI Violent Crimes, FBI Child Exploitation, Secret Service)
 - a. Review and take possible action on reports
6. AB 2336 (Friedman) Speed Safety System Pilot Program – DOT/Chair – evaluation of proposed bill solely as to potential privacy impact
 - a. Review and take possible action on draft resolution
7. Surveillance Equipment Ordinance – OPD – Crime Analysis Software
 - a. Review and take possible action on Impact Report and proposed Use Policy
8. Surveillance Equipment Ordinance – DVP – Apricot 360 database
 - a. Review and take possible action on Impact Report and proposed Use Policy
9. Surveillance Equipment Ordinance – EDW – East Oakland Security Camera Proposal
 - a. Review and take possible action on Impact Report and proposed Use Policy
10. Surveillance Equipment Ordinance – OPD – Annual Reports (Automated License Plate Readers, Cell-Site Simulator, Biometric Crime Lab, Forensic Logic/Coplink, GPS Tag Tracker, ShotSpotter, Live Stream Camera, Mobile Fingerprint ID, Unmanned Aerial Vehicles/Drones)
 - a. Review and take possible action on the reports

OAKLAND PRIVACY ADVISORY COMMISSION

RESOLUTION NO. 2

ADOPT A RESOLUTION DETERMINING THAT CONDUCTING IN-PERSON MEETINGS OF THE PRIVACY ADVISORY COMMISSION AND ITS COMMITTEES WOULD PRESENT IMMINENT RISKS TO ATTENDEES' HEALTH, AND ELECTING TO CONTINUE CONDUCTING MEETINGS USING TELECONFERENCING IN ACCORDANCE WITH CALIFORNIA GOVERNMENT CODE SECTION 54953(e), A PROVISION OF AB-361.

WHEREAS, on March 4, 2020, Governor Gavin Newsom declared a state of emergency related to COVID-19, pursuant to Government Code Section 8625, and such declaration has not been lifted or rescinded. *See* <https://www.gov.ca.gov/wp-content/uploads/2020/03/3.4.20-Coronavirus-SOE-Proclamation.pdf>; and

WHEREAS, on March 9, 2020, the City Administrator in their capacity as the Director of the Emergency Operations Center (EOC), issued a proclamation of local emergency due to the spread of COVID-19 in Oakland, and on March 12, 2020, the City Council passed Resolution No. 88075 C.M.S. ratifying the proclamation of local emergency pursuant to Oakland Municipal Code (O.M.C.) section 8.50.050(C); and

WHEREAS, City Council Resolution No. 88075 remains in full force and effect to date; and

WHEREAS, the Centers for Disease Control (CDC) recommends physical distancing of at least six (6) feet whenever possible, avoiding crowds, and avoiding spaces that do not offer fresh air from the outdoors, particularly for people who are not fully vaccinated or who are at higher risk of getting very sick from COVID-19. *See* <https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html>; and

WHEREAS, the CDC recommends that people who live with unvaccinated people avoid activities that make physical distancing hard. *See* <https://www.cdc.gov/coronavirus/2019-ncov/your-health/about-covid-19/caring-for-children/families.html>; and

WHEREAS, the CDC recommends that older adults limit in-person interactions as much as possible, particularly when indoors. *See* <https://www.cdc.gov/aging/covid19/covid19-older-adults.html>; and

WHEREAS, the CDC, the California Department of Public Health, and the Alameda County Public Health Department all recommend that people experiencing COVID-19

symptoms stay home. See <https://www.cdc.gov/coronavirus/2019-ncov/if-you-are-sick/steps-when-sick.html>; and

WHEREAS, persons without symptoms may be able to spread the COVID-19 virus. See <https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html>; and

WHEREAS, fully vaccinated persons who become infected with the COVID-19 Delta variant can spread the virus to others. See <https://www.cdc.gov/coronavirus/2019-ncov/vaccines/fully-vaccinated.html>; and

WHEREAS, the City's public-meeting facilities are indoor facilities that do not ensure circulation of fresh / outdoor air, particularly during periods of cold and/or rainy weather, and were not designed to ensure that attendees can remain six (6) feet apart; and

WHEREAS, holding in-person meetings would encourage community members to come to City facilities to participate in local government, and some of them would be at high risk of getting very sick from COVID-19 and/or would live with someone who is at high risk; and

WHEREAS, in-person meetings would tempt community members who are experiencing COVID-19 symptoms to leave their homes in order to come to City facilities and participate in local government; and

WHEREAS, attendees would use ride-share services and/or public transit to travel to in-person meetings, thereby putting them in close and prolonged contact with additional people outside of their households; and

WHEREAS, on October 7, 2021, the Privacy Advisory Commission adopted a resolution determining that conducting in-person meetings would present imminent risks to attendees' health, and electing to continue conducting meetings using teleconferencing in accordance with California Government Code Section 54953(e), a provision of AB-361; now therefore be it:

RESOLVED: that the Privacy Advisory Commission finds and determines that the foregoing recitals are true and correct and hereby adopts and incorporates them into this resolution; and be it

FURTHER RESOLVED: that, based on these determinations and consistent with federal, state and local health guidance, the Privacy Advisory Commission renews its determination that conducting in-person meetings would pose imminent risks to the health of attendees; and be it

FURTHER RESOLVED: that the Privacy Advisory Commission firmly believes that the community's health and safety and the community's right to participate in local government, are both critically important, and is committed to balancing the two by continuing to use teleconferencing to conduct public meetings, in accordance with California Government Code Section 54953(e), a provision of AB-361; and be it

FURTHER RESOLVED: that the Privacy Advisory Commission will renew these (or similar) findings at least every thirty (30) days in accordance with California Government Code section 54953(e) until the state of emergency related to COVID-19 has been lifted, or the Privacy Advisory Commission finds that in-person meetings no longer pose imminent risks to the health of attendees, whichever occurs first.

AMENDED IN ASSEMBLY APRIL 21, 2022

AMENDED IN ASSEMBLY MARCH 22, 2022

CALIFORNIA LEGISLATURE—2021–22 REGULAR SESSION

ASSEMBLY BILL

No. 2336

Introduced by Assembly Members Friedman and Ting
(Coauthor: Assembly Member Wicks)

February 16, 2022

An act to amend, repeal, and add Section 70615 of the Government Code, ~~and to amend, repeal, and add Section 9800 of,~~ and to add and repeal Article 3 (commencing with Section 22425) of Chapter 7 of Division 11 of, the Vehicle Code, relating to vehicles.

LEGISLATIVE COUNSEL'S DIGEST

AB 2336, as amended, Friedman. Vehicles: Speed Safety System Pilot Program.

Existing law establishes a basic speed law that prohibits a person from driving a vehicle upon a highway at a speed greater than is reasonable or prudent given the weather, visibility, traffic, and highway ~~conditions,~~ *conditions* and in no event at a speed that endangers the safety of persons or property.

This bill would authorize, until January 1, 2028, the Cities of Los Angeles, Oakland, San Jose, ~~and Glendale, one southern California city,~~ *and Palm Springs*, and the City and County of San Francisco, to establish the Speed Safety System Pilot Program if the system meets specified requirements. The bill would require the participating cities or city and county to adopt a Speed Safety System Use Policy and a Speed Safety System Impact Report before implementing the program, and would require the city or city and county to engage in a public

information campaign at least 30 days before implementation of the program, including information relating to when the systems would begin detecting violations and where the systems would be utilized. The bill would require the participating cities or city and county to issue warning notices rather than notices of violations for violations detected within the first ~~30~~ 60 calendar days of the program. The bill would require the participating cities or city and county to develop uniform guidelines for, among other things, the processing and storage of confidential information. The bill would designate all photographic, video, or other visual or administrative ~~records~~ *records, not including data about the number of violations issued or the speeds at which they were issued for*, made by a system as confidential, and would only authorize public agencies to use and allow access to these records for specified purposes.

This bill would specify that any violation of a speed law recorded by a speed safety system authorized by these provisions would be subject only to the provided civil penalties. The bill would, among other things, provide for the issuance of a notice of violation, an initial review, an administrative hearing, and an appeals process, as specified, for a violation under this program. The bill would require any program created pursuant to these provisions to offer a diversion program for indigent speed safety system violation recipients, as specified. The bill would require a city or city and county participating in the pilot program to submit reports to the Legislature, as specified, to evaluate the speed safety system to determine the ~~system's~~ *system's* impact on street safety and economic impact on the communities where the system is utilized.

Existing law establishes a \$25 filing fee for specified appeals and petitions.

This bill would require a \$25 filing fee for an appeal challenging a notice of violation issued as a result of a speed safety system until January 1, 2028.

~~Existing law establishes that payments for specified charges and penalties, including penalties for offenses relating to the parking of a vehicle, constitute a lien on the vehicle and on any other vehicle owned by the owner of that vehicle.~~

~~This bill, until January 1, 2028, would also include as constituting a lien on those vehicles payments for penalties for offenses detected by a speed safety system for which a notice of violation has been served on the owner or recipient of a reissued citation and any delinquent fees added to the penalty.~~

This bill would make legislative findings and declarations as to the necessity of a special statute for the Cities of Los Angeles, Oakland, San Jose, and Glendale, ~~one southern California city,~~ and Palm Springs and the City and County of San Francisco.

Existing constitutional provisions require that a statute that limits the right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.

This bill would make legislative findings to that effect.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: no.

The people of the State of California do enact as follows:

- 1 SECTION 1. The Legislature finds and declares all of the
2 following:
- 3 (a) Speed is a major factor in traffic collisions that result in
4 fatalities or injuries.
- 5 (b) State and local agencies employ a variety of methods to
6 reduce speeding, including traffic engineering, education, and
7 enforcement.
- 8 (c) Traffic speed enforcement is critical to efforts in California
9 to reduce factors that contribute to traffic collisions that result in
10 fatalities or injuries.
- 11 (d) However, traditional enforcement methods have had a
12 well-documented disparate impact on communities of color, and
13 implicit or explicit racial bias in police traffic stops puts drivers
14 of color at risk.
- 15 (e) Additional tools, including speed safety systems, are
16 available to assist cities and the state in addressing excessive
17 speeding and speed-related crashes.
- 18 (f) Speed safety systems offer a high rate of detection, and, in
19 conjunction with education and traffic engineering, can
20 significantly reduce speeding, improve traffic safety, and prevent
21 traffic-related fatalities and injuries, including roadway worker
22 fatalities.
- 23 (g) Multiple speed safety system programs implemented in other
24 states and cities outside of California have proven successful in
25 reducing speeding and addressing traffic safety concerns.

1 (h) The Transportation Agency’s “CalSTA Report of Findings:
2 AB 2363 Zero Traffic Fatalities Task Force,” issued in January
3 2020, concluded that international and domestic studies show that
4 speed safety systems are an effective countermeasure to speeding
5 that can deliver meaningful safety improvements, and identified
6 several policy considerations that speed safety system program
7 guidelines could consider.

8 (i) In a 2017 study, the National Transportation Safety Board
9 (NTSB) analyzed studies of speed safety system programs, and
10 found they offered significant safety improvements in the forms
11 of reduction in mean speeds, reduction in the likelihood of speeding
12 more than 10 miles per hour over the posted speed limit, and
13 reduction in the likelihood that a crash involved a severe injury or
14 fatality. The same study recommended that all states remove
15 obstacles to speed safety system programs to increase the use of
16 this proven approach, and notes that programs should be explicitly
17 authorized by state legislation without operational and location
18 restrictions.

19 (j) The National Highway Traffic Safety Administration
20 (NHTSA) gives speed safety systems the maximum 5-star
21 effectiveness rating. NHTSA issued speed enforcement camera
22 systems operational guidelines in 2008, and is expected to release
23 revised guidelines in 2021 that should further inform the
24 development of state guidelines.

25 (k) Speed safety systems can advance equity by improving
26 reliability and fairness in traffic enforcement while making
27 speeding enforcement more predictable, effective, and broadly
28 implemented, all of which helps change driver behavior.

29 (l) Enforcing speed limits using speed safety systems on streets
30 where speeding drivers create dangerous roadway environments
31 is a reliable and cost-effective means to prevent further fatalities
32 and injuries.

33 SEC. 2. Section 70615 of the Government Code is amended
34 to read:

35 70615. The fee for filing any of the following appeals to the
36 superior court is twenty-five dollars (\$25):

37 (a) An appeal of a local agency’s decision regarding an
38 administrative fine or penalty under Section 53069.4.

39 (b) An appeal under Section 40230 of the Vehicle Code of an
40 administrative agency’s decision regarding a parking violation.

1 (c) An appeal under Section 99582 of the Public Utilities Code
2 of a hearing officer's determination regarding an administrative
3 penalty for fare evasion or a passenger conduct violation.

4 (d) A petition under Section 186.35 of the Penal Code
5 challenging a law enforcement agency's inclusion of a person's
6 information in a shared gang database.

7 (e) An appeal under Section 22428 of the Vehicle Code of a
8 hearing officer's determination regarding a civil penalty for an
9 automated speed violation, as defined in Section 22425 of the
10 Vehicle Code.

11 (f) This section shall remain in effect only until January 1, 2028,
12 and as of that date is repealed.

13 SEC. 3. Section 70615 is added to the Government Code, to
14 read:

15 70615. The fee for filing any of the following appeals to the
16 superior court is twenty-five dollars (\$25):

17 (a) An appeal of a local agency's decision regarding an
18 administrative fine or penalty under Section 53069.4.

19 (b) An appeal under Section 40230 of the Vehicle Code of an
20 administrative agency's decision regarding a parking violation.

21 (c) An appeal under Section 99582 of the Public Utilities Code
22 of a hearing officer's determination regarding an administrative
23 penalty for fare evasion or a passenger conduct violation.

24 (d) A petition under Section 186.35 of the Penal Code
25 challenging a law enforcement agency's inclusion of a person's
26 information in a shared gang database.

27 (e) This section shall become operative on January 1, 2028.

28 SEC. 4. ~~Section 9800 of the Vehicle Code is amended to read:~~

29 ~~9800. (a) Payments for any of the following, and any interest,
30 penalties, or service fees added thereto, required to register or
31 transfer the registration of a vehicle, constitute a lien on the vehicle
32 on which they are due or which was involved in the offense, and
33 on any other vehicle owned by the owner of that vehicle:~~

34 ~~(1) Registration fees.~~

35 ~~(2) Transfer fees.~~

36 ~~(3) License fees.~~

37 ~~(4) Use taxes.~~

38 ~~(5) Penalties for offenses relating to the standing or parking of
39 a vehicle for which a notice of parking violation has been served~~

1 on the owner, and any administrative service fee added to the
2 penalty.

3 ~~(6) Any court-imposed fine or penalty assessment, and any~~
4 ~~administrative service fee added thereto, which is subject to~~
5 ~~collection by the department.~~

6 ~~(7) Penalties for offenses detected by a speed safety system, as~~
7 ~~defined in Section 22425, for which a notice of violation has been~~
8 ~~served on the owner or recipient of a reissued citation and any~~
9 ~~delinquent fees added to the penalty.~~

10 ~~(b) Notwithstanding subdivision (a), if a person is cited for a~~
11 ~~foreign registered auxiliary dolly, semitrailer, or trailer having~~
12 ~~been operated without current year registration or valid California~~
13 ~~permits or registration, an amount equal to the minimum~~
14 ~~registration fees or transfer fees, and any penalty added thereto,~~
15 ~~from the date they became due, shall, by election of the power unit~~
16 ~~operator, constitute a lien upon the California registered power~~
17 ~~unit which was pulling the dolly, semitrailer, or trailer. However,~~
18 ~~this subdivision is not applicable if the citation is issued at a scale~~
19 ~~operated by the Department of the California Highway Patrol and~~
20 ~~registration for the vehicle can be issued there immediately upon~~
21 ~~payment of the fees due.~~

22 ~~(c) Every lien arising under this section expires three years from~~
23 ~~the date the fee, tax, or parking penalty first became due unless~~
24 ~~the lien is perfected pursuant to subdivision (d).~~

25 ~~(d) A lien is perfected when a notice is mailed to the registered~~
26 ~~and legal owners at the addresses shown in the department's~~
27 ~~records and the lien is recorded on the electronic vehicle~~
28 ~~registration records of the department. A perfected lien shall expire~~
29 ~~five years from the date of perfection.~~

30 ~~(e) Employees and members of the Department of the California~~
31 ~~Highway Patrol assigned to commercial vehicle scale facilities~~
32 ~~may possess and sell trip permits approved by the Department of~~
33 ~~Motor Vehicles.~~

34 ~~(f) This section shall remain in effect only until January 1, 2028,~~
35 ~~and as of that date is repealed, unless a later enacted statute that~~
36 ~~is enacted before January 1, 2028, deletes or extends that date.~~

37 ~~SEC. 5. Section 9800 is added to the Vehicle Code, to read:~~

38 ~~9800. (a) Payments for any of the following, and any interest,~~
39 ~~penalties, or service fees added thereto, required to register or~~
40 ~~transfer the registration of a vehicle, constitute a lien on the vehicle~~

1 on which they are due or which was involved in the offense, and
2 on any other vehicle owned by the owner of that vehicle:

3 ~~(1) Registration fees.~~

4 ~~(2) Transfer fees.~~

5 ~~(3) License fees.~~

6 ~~(4) Use taxes.~~

7 ~~(5) Penalties for offenses relating to the standing or parking of~~
8 ~~a vehicle for which a notice of parking violation has been served~~
9 ~~on the owner, and any administrative service fee added to the~~
10 ~~penalty.~~

11 ~~(6) Any court-imposed fine or penalty assessment, and any~~
12 ~~administrative service fee added thereto, which is subject to~~
13 ~~collection by the department.~~

14 ~~(b) Notwithstanding subdivision (a), if a person is cited for a~~
15 ~~foreign registered auxiliary dolly, semitrailer, or trailer having~~
16 ~~been operated without current year registration or valid California~~
17 ~~permits or registration, an amount equal to the minimum~~
18 ~~registration fees or transfer fees, and any penalty added thereto,~~
19 ~~from the date they became due, shall, by election of the power unit~~
20 ~~operator, constitute a lien upon the California registered power~~
21 ~~unit which was pulling the dolly, semitrailer, or trailer. However,~~
22 ~~this subdivision is not applicable if the citation is issued at a scale~~
23 ~~operated by the Department of the California Highway Patrol and~~
24 ~~registration for the vehicle can be issued there immediately upon~~
25 ~~payment of the fees due.~~

26 ~~(c) Every lien arising under this section expires three years from~~
27 ~~the date the fee, tax, or parking penalty first became due unless~~
28 ~~the lien is perfected pursuant to subdivision (d).~~

29 ~~(d) A lien is perfected when a notice is mailed to the registered~~
30 ~~and legal owners at the addresses shown in the department's~~
31 ~~records and the lien is recorded on the electronic vehicle~~
32 ~~registration records of the department. A perfected lien shall expire~~
33 ~~five years from the date of perfection.~~

34 ~~(e) Employees and members of the Department of the California~~
35 ~~Highway Patrol assigned to commercial vehicle scale facilities~~
36 ~~may possess and sell trip permits approved by the Department of~~
37 ~~Motor Vehicles.~~

38 ~~(f) This section shall become operative on January 1, 2028.~~

1 ~~SEC. 6.~~

2 SEC. 4. Article 3 (commencing with Section 22425) is added
3 to Chapter 7 of Division 11 of the Vehicle Code, to read:

4

5 Article 3. Speed Safety System Pilot Program

6

7 22425. (a) As used in this article, the following definitions
8 apply:

9 (1) “Automated speed violation” means a violation of a speed
10 law detected by a speed safety system operated pursuant to this
11 article.

12 (2) “Indigent” has the same meaning as defined in subdivision
13 (c) of Section 40220.

14 (3) “Local department of transportation” means a city or city
15 and county’s department of transportation or, if a city or city and
16 county does not have a department of transportation, their
17 administrative division, including, but not limited to, a public
18 works department that administers transportation and traffic matters
19 under this code.

20 (4) “Speed safety system” or “system” means a fixed or mobile
21 radar or laser system or any other electronic device that utilizes
22 automated equipment to detect a violation of speeding laws and
23 is designed to obtain a clear photograph, video recording, or other
24 visual image of a vehicle license plate.

25 (b) (1) ~~The Cities of Los Angeles, Oakland, San Jose, and~~
26 ~~Glendale, one southern California city, and Palm Springs,~~ and the
27 City and County of San Francisco, may establish a program
28 utilizing a speed safety system for speed enforcement, to be
29 operated by a local department of transportation, in the following
30 areas:

31 (A) On a street meeting the standards of a safety corridor under
32 Section 22358.7.

33 (B) On a street a local authority has determined to have had a
34 high number of incidents for motor vehicle speed contests or motor
35 vehicle exhibitions of speed.

36 (C) School zones, subject to subdivision (d).

37 (2) A municipality operating a speed safety system pilot program
38 under this article may have speed safety systems operational on
39 no more than 15 percent of the municipality’s streets at any time
40 during the pilot program.

1 (3) (A) A municipality operating a speed safety pilot program
2 under this article may have the following number of speed safety
3 systems operational at any time during the pilot program:

4 (i) For a jurisdiction with a population over 3,000,000, no more
5 than 125 systems.

6 (ii) For a jurisdiction with a population between 800,000 and
7 3,000,000, inclusive, no more than 33 systems.

8 (iii) For a jurisdiction with a population of 300,000 up to
9 800,000, no more than 18 systems.

10 (iv) For a jurisdiction with a population of less than 300,000,
11 no more than nine systems.

12 (B) For purposes of this paragraph, a “speed safety system”
13 may include up to two fixed or mobile radar or laser systems at
14 the same location in order to detect speed violations on two-way
15 or multidirectional streets.

16 (c) The Speed Safety System Pilot Program shall not be operated
17 on any California state route, including all freeways and
18 expressways, United States Highway, Interstate Highway Highway,
19 or any public road in an unincorporated county where the
20 Commissioner of the California Highway Patrol has full
21 responsibility and primary jurisdiction for the administration and
22 enforcement of the laws, and for the investigation of traffic
23 accidents, pursuant to Section 2400.

24 (d) If a school zone has a posted speed limit of 30 miles per
25 hour or higher when children are not present, a city or city and
26 county may operate a speed safety system *up to* two hours before
27 the regular school session begins and *up to* two hours after regular
28 school session concludes. *For these school zones, flashing beacons*
29 *activated by a time clock, other automatic device, or manual*
30 *activation shall be installed on the school zone speed limit sign*
31 *and active to indicate the times during which the school zone speed*
32 *limit is enforced with a speed safety system.*

33 (e) A speed safety system for speed limit enforcement may be
34 utilized pursuant to subdivision (b) if the program meets all of the
35 following requirements:

36 (1) Clearly identifies the presence of the speed safety system
37 by signs stating “Photo Enforced,” along with the posted speed
38 limit within 500 feet of the system. The signs shall be visible to
39 traffic traveling on the street from the direction of travel for which
40 the system is utilized, and shall be posted at all locations as may

1 be determined necessary by the Department of Transportation
2 through collaboration with the California Traffic Control Devices
3 Committee.

4 (2) Identifies the streets or portions of streets that have been
5 approved for enforcement using a speed safety system and the
6 hours of enforcement on the municipality's internet website, which
7 shall be updated whenever the municipality changes locations of
8 enforcement.

9 (3) Ensures that the speed safety system is regularly inspected
10 and certifies that the system is installed and operating properly.
11 Each camera unit shall be calibrated in accordance with the
12 manufacturer's instructions, and at least once per year by an
13 independent calibration laboratory. Documentation of the regular
14 inspection, operation, and calibration of the system shall be retained
15 until the date on which the system has been permanently removed
16 from use.

17 (4) Utilizes fixed or mobile speed safety systems that provide
18 real-time notification when violations are detected.

19 (f) Prior to enforcing speed laws utilizing speed safety systems,
20 the city or city and county shall do both of the following:

21 (1) Administer a public information campaign for at least 30
22 calendar days prior to the commencement of the program, which
23 shall include public announcements in major media outlets and
24 press releases. The public information campaign shall include the
25 draft Speed Safety System Use Policy pursuant to subdivision (g),
26 the Speed Safety System Impact Report pursuant to subdivision
27 (h), information on when systems will begin detecting violations,
28 the streets, or portions of streets, where systems will be utilized,
29 and the city's internet website, where additional information about
30 the program can be obtained. Notwithstanding the above, no further
31 public announcement by the municipality shall be required for
32 additional systems that may be added to the program.

33 (2) Issue warning notices rather than notices of violation for
34 violations detected by the speed safety systems during the first-~~30~~
35 ~~60~~ calendar days of enforcement under the program. If additional
36 systems are utilized on additional streets after the initial program
37 implementation, the city or city and county shall issue warning
38 notices rather than notices of violation for violations detected by
39 the new speed safety systems during the first-~~30~~ ~~60~~ calendar days
40 of enforcement for the additional streets added to the program.

1 (g) The local governing body shall adopt a Speed Safety System
2 Use Policy before entering into an agreement regarding a speed
3 safety system, purchasing or leasing equipment for a program, or
4 implementing a program. The Speed Safety System Use Policy
5 shall include the specific purpose for the system, the uses that are
6 authorized, the rules and processes required prior to that use, and
7 the uses that are prohibited. The policy shall include the data or
8 information that can be collected by the speed safety system and
9 the individuals who can access or use the collected information,
10 and the rules and processes related to the access or use of the
11 information. The policy shall also include provisions for protecting
12 data from unauthorized access, data retention, public access,
13 third-party data sharing, training, auditing, and oversight to ensure
14 compliance with the Speed Safety System Use Policy. The Speed
15 Safety System Use Policy shall be made available for public
16 review, including, but not limited to, by posting it on the local
17 governing body's internet website at least 30 calendar days prior
18 to adoption by the local governing body.

19 (h) (1) The local governing body also shall approve a Speed
20 Safety System Impact Report prior to implementing a program.
21 The Speed Safety System Impact Report shall include all of the
22 following information:

23 (A) Assessment of potential impact of the speed safety system
24 on civil liberties and civil rights and any plans to safeguard those
25 public rights.

26 (B) Description of the speed safety system and how it works.

27 (C) Fiscal costs for the speed safety system, including program
28 establishment costs, ongoing costs, and program funding.

29 (D) If potential deployment locations of systems are
30 predominantly in low-income neighborhoods, a determination of
31 why these locations experience high fatality and injury collisions
32 due to unsafe speed.

33 (E) Locations where the system may be deployed and traffic
34 data for these locations.

35 (F) Proposed purpose of the speed safety system.

36 (2) The Speed Safety System Impact Report shall be made
37 available for public review at least 30 calendar days prior to
38 adoption by the governing body.

39 (3) The local governing body shall consult and work
40 collaboratively with relevant local stakeholder organizations,

1 including racial equity, privacy protection, and economic justice
2 groups, in developing the Speed Safety System Use Policy and
3 Speed Safety System Impact Report.

4 (i) The municipality shall develop uniform guidelines for both
5 of the following:

6 (1) The screening and issuing of notices of violation.

7 (2) The processing and storage of confidential information and
8 procedures to ensure compliance with confidentiality requirements.

9 (j) Notices of violation issued pursuant to this section shall
10 include a clear photograph, video recording, or other visual image
11 of the license plate and rear of the vehicle only, the Vehicle Code
12 violation, the camera location, and the date and time when the
13 violation occurred. Notices of violation shall exclude images of
14 the rear window area of the vehicle.

15 (k) The photographic, video, or other visual evidence stored by
16 a speed safety system does not constitute an out-of-court hearsay
17 statement by a declarant under Division 10 (commencing with
18 Section 1200) of the Evidence Code.

19 (l) (1) Notwithstanding Sections 6253 and 6262 of the
20 Government Code, or any other law, photographic, video, or other
21 visual or administrative records made by a system shall be
22 confidential. Public agencies shall use and allow access to these
23 records only for the purposes authorized by this article or to assess
24 the impacts of the system. *Data about the number of violations*
25 *issued and the speeds at which they were issued for is not*
26 *considered administrative records required to be confidential by*
27 *this section.*

28 (2) Confidential information obtained from the Department of
29 Motor Vehicles for the administration of speed safety systems and
30 enforcement of this article shall be held confidential, and shall not
31 be used for any other purpose.

32 (3) Except for court records described in Section 68152 of the
33 Government Code, or as provided in paragraph (4), the confidential
34 records and evidence described in paragraphs (1) and (2) may be
35 retained for up to 60 days after final disposition of the notice of
36 violation. The municipality may adopt a retention period of less
37 than 60 days in the Speed Safety System Use Policy.
38 Administrative records described in paragraph (1) may be retained
39 for up to 120 days after final disposition of the notice of violation.
40 Notwithstanding any other law, the confidential records and

1 evidence shall be destroyed in a manner that maintains the
2 confidentiality of any person included in the record or evidence.

3 (4) Notwithstanding Section 26202.6 of the Government Code,
4 photographic, video, or other visual evidence that is obtained from
5 a speed safety system that does not contain evidence of a speeding
6 violation shall be destroyed within five business days after the
7 evidence was first obtained. The use of facial recognition
8 technology in conjunction with a speed safety system shall be
9 prohibited.

10 (5) Information collected and maintained by a municipality
11 using a speed safety system shall only be used to administer ~~an~~ a
12 program, and shall not be disclosed to any other persons, including,
13 but not limited to, any other state or federal government agency
14 or official for any other purpose, except as required by state or
15 federal law, court order, or in response to a subpoena in an
16 individual case or proceeding.

17 (m) Notwithstanding subdivision (l), the registered owner or an
18 individual identified by the registered owner as the driver of the
19 vehicle at the time of the alleged violation shall be permitted to
20 review the photographic, video, or visual evidence of the alleged
21 violation.

22 (n) A contract between the municipality and a manufacturer or
23 supplier of speed safety systems shall allow the local authority to
24 purchase materials, lease equipment, and contract for processing
25 services from the manufacturer or supplier based on the services
26 rendered on a monthly schedule or another schedule agreed upon
27 by the municipality and contractor. The contract shall not include
28 provisions for payment or compensation based on the number of
29 notices of violation issued by a designated municipal employee,
30 or as a percentage of revenue generated, from the use of the system.
31 The contract shall include a provision that all data collected from
32 the speed safety systems is confidential, and shall prohibit the
33 manufacturer or supplier of speed safety systems from sharing,
34 repurposing, or monetizing collected data, except as specifically
35 authorized in this article. The municipality shall oversee and
36 maintain control over all enforcement activities, including the
37 determination of when a notice of violation should be issued.

38 (o) Notwithstanding subdivision (n), a municipality may contract
39 with a vendor for the processing of notices of violation after a
40 designated municipal employee has issued a notice of violation.

1 The vendor shall be a separate legal and corporate entity from, and
2 unrelated or affiliated in any manner with, the manufacturer or
3 supplier of speed safety systems used by the municipality. Any
4 contract between the municipality and a vendor to provide
5 processing services may include a provision for the payment of
6 compensation based on the number of notices of violation
7 processed by the vendor.

8 (p) (1) A speed safety system shall no longer be operated on
9 any given street if within the first 18 months of installation of a
10 system, at least one of the following thresholds has not been met:

11 (A) Percentage of automated speed violations decreased by at
12 least 25 percent.

13 (B) Percentage of violators who received two or more violations
14 decreased by at least 50 percent.

15 (2) This subdivision does not apply if a city or city and county
16 adds traffic-calming measures to the street. “Traffic-calming
17 measures” include, but are not limited to:

18 (A) Bicycle lanes.

19 (B) Chicanes.

20 (C) Chokers.

21 (D) Curb extensions.

22 (E) Median islands.

23 (F) Raised crosswalks.

24 (G) Road diets.

25 (H) Roundabouts.

26 (I) Speed humps or speed tables.

27 (J) Traffic circles.

28 (3) A city or city and county may continue to operate a speed
29 safety system with a fixed or mobile vehicle speed feedback sign
30 while traffic-calming measures are being planned or constructed,
31 but shall halt their use if construction has not begun within two
32 years.

33 (4) If the percentage of violations has not decreased by the
34 metrics identified pursuant to paragraph (1) within one year after
35 traffic-calming measures have completed construction, a city or
36 county shall either construct additional traffic-calming measures
37 or cease operation of the system on that street.

38 22426. (a) Notwithstanding any other law, a violation of
39 Section 22350, or any other speed law pursuant to this chapter that
40 is recorded by a speed safety system authorized pursuant to Section

1 22425 shall be subject only to a civil penalty, as provided in
2 subdivision (c), and shall not result in the department suspending
3 or revoking the privilege of a violator to drive a motor vehicle or
4 in a violation point being assessed against the violator.

5 (b) The speed safety system shall capture images of the rear
6 license plate of vehicles that are traveling 11 miles per hour or
7 more over the posted speed limit and notices of violation shall
8 only be issued to vehicles based on that evidence.

9 (c) A civil penalty shall be assessed as follows:

10 (1) Fifty dollars (\$50) for a speed violation from 11 up to 15
11 miles per hour over the posted speed limit.

12 (2) One hundred dollars (\$100) for a speed violation from 16
13 up to 25 miles per hour over the posted speed limit.

14 (3) Two hundred dollars (\$200) for a speed violation of 26 miles
15 per hour or more over the posted speed limit, unless paragraph (4)
16 applies.

17 (4) Five hundred dollars (\$500) for traveling at a speed of 100
18 miles per hour or greater.

19 (d) A civil penalty shall not be assessed against an authorized
20 emergency vehicle.

21 (e) The written notice of violation shall be issued to the
22 registered owner of the vehicle within 15 calendar days of the date
23 of the violation. The notice of violation shall include all of the
24 following information:

25 (1) The violation, including reference to the speed law that was
26 violated.

27 (2) The date, approximate time, and location where the violation
28 occurred.

29 (3) The vehicle license number and the name and address of the
30 registered owner of the vehicle.

31 (4) A statement that payment is required to be made no later
32 than 30 calendar days from the date of mailing of the notice of
33 violation, or that the violation may be contested pursuant to Section
34 22427.

35 (5) The amount of the civil penalty due for that violation and
36 the procedures for the registered owner, lessee, or rentee to pay
37 the civil penalty or to contest the notice of violation.

38 (6) An affidavit of nonliability, and information of what
39 constitutes nonliability, information as to the effect of executing
40 the affidavit, and instructions for returning the affidavit to the

1 processing agency. If the affidavit of nonliability is returned to the
2 processing agency within 30 calendar days of the mailing of the
3 notice of violation, together with proof of a written lease or rental
4 agreement between a bona fide rental or leasing company and its
5 customer that identifies the rentee or lessee, the processing agency
6 shall serve or mail a notice of violation to the rentee or lessee
7 identified in the affidavit of nonliability.

8 (f) Mobile radar or laser systems shall not be used until at least
9 two years after the installation of the first fixed radar or laser
10 system.

11 (g) (1) Revenues derived from any program utilizing a speed
12 safety system for speed limit enforcement shall first be used to
13 recover program costs. Program costs include, but are not limited
14 to, the construction of ~~traffic-calming~~ *traffic-calming* measures for
15 the purposes of complying with subdivision (p) of Section 22425,
16 the installation of speed safety systems, the adjudication of
17 violations, and reporting requirements as specified in this section.

18 (2) Jurisdictions shall maintain their existing commitment of
19 local funds for *traffic-calming* measures in order to remain
20 authorized to participate in the pilot program, and shall annually
21 expend not less than the annual average of expenditures for
22 *traffic-calming* measures during the 2016–17, 2017–18, and
23 2018–19 fiscal years. For purposes of this subdivision, in
24 calculating average expenditures on *traffic-calming* measures,
25 restricted funds that may not be available on an ongoing basis,
26 including those from voter-approved bond issuances or tax
27 measures, shall not be included. Any excess revenue shall be used
28 for ~~traffic-calming~~ *traffic-calming* measures within three years. If
29 *traffic-calming* measures are not planned or constructed after the
30 third year, excess revenue shall revert to the Active Transportation
31 Program established pursuant to Chapter 8 (commencing with
32 Section 2380) of the Streets and Highways Code, to be allocated
33 by the California Transportation Commission pursuant to Section
34 2381 of the Streets and Highways Code.

35 22427. (a) For a period of 30 calendar days from the mailing
36 of a notice of violation, a person may request an initial review of
37 the notice by the issuing agency. The request may be made by
38 telephone, in writing, electronically, or in person. There shall be
39 no charge for this review. If, following the initial review, the
40 issuing agency is satisfied that the violation did not occur, or that

1 extenuating circumstances make dismissal of the notice of violation
2 appropriate in the interest of justice, the issuing agency shall cancel
3 the notice of violation. The issuing agency shall advise the
4 processing agency, if any, of the cancellation. The issuing agency
5 or the processing agency shall mail the results of the initial review
6 to the person contesting the notice, and, if cancellation of the notice
7 does not occur following that review, include a reason for that
8 denial, notification of the ability to request an administrative
9 hearing, and notice of the procedure adopted pursuant to paragraph
10 (2) of subdivision (b) for waiving prepayment of the civil penalty
11 based upon an inability to pay.

12 (b) (1) If the person contesting the notice of violation is
13 dissatisfied with the results of the initial review, the person may,
14 no later than 21 calendar days following the mailing of the results
15 of the issuing agency's initial review, request an administrative
16 hearing of the violation. The request may be made by telephone,
17 in writing, electronically, or in person.

18 (2) The person requesting an administrative hearing shall pay
19 the amount of the civil penalty to the processing agency. The
20 issuing agency shall adopt a written procedure to allow a person
21 to request an administrative hearing without payment of the civil
22 penalty upon satisfactory proof of an inability to pay the amount
23 due.

24 (3) The administrative hearing shall be held within 90 calendar
25 days following the receipt of a request for an administrative
26 hearing. The person requesting the hearing may request one
27 continuance, not to exceed 21 calendar days.

28 (c) The administrative hearing process shall include all of the
29 following:

30 (1) The person requesting a hearing shall have the choice of a
31 hearing by mail, video conference, or in person. An in-person
32 hearing shall be conducted within the jurisdiction of the issuing
33 agency.

34 (2) If the person requesting a hearing is a minor, that person
35 shall be permitted to appear at a hearing or admit responsibility
36 for the automated speed violation without the appointment of a
37 guardian. The processing agency may proceed against the minor
38 in the same manner as against an adult.

39 (3) The administrative hearing shall be conducted in accordance
40 with written procedures established by the issuing agency and

1 approved by the governing body or chief executive officer of the
2 issuing agency. The hearing shall provide an independent,
3 objective, fair, and impartial review of contested automated speed
4 violations.

5 (4) (A) The issuing agency's governing body or chief executive
6 officer shall appoint or contract with qualified independent
7 examiners or administrative hearing providers that employ qualified
8 independent examiners to conduct the administrative hearings.
9 Examiners shall demonstrate the qualifications, training, and
10 objectivity necessary to conduct a fair and impartial review. The
11 examiner shall be separate and independent from the notice of
12 violation collection or processing function. An examiner's
13 continued employment, performance evaluation, compensation,
14 and benefits shall not, directly or indirectly, be linked to the amount
15 of civil penalties collected by the examiner or the number or
16 percentage of violations upheld by the examiner.

17 (B) (i) Examiners shall have a minimum of 20 hours of training.
18 The examiner is responsible for the costs of the training. The
19 issuing agency may reimburse the examiner for those costs.
20 Training may be provided through any of the following:

21 (I) An accredited college or university.

22 (II) A program conducted by the Commission on Peace Officer
23 Standards and Training.

24 (III) A program conducted by the American Arbitration
25 Association or a similar organization.

26 (IV) Any program approved by the governing body or chief
27 executive officer of the issuing agency, including a program
28 developed and provided by, or for, the agency.

29 (ii) Training programs may include topics relevant to the
30 administrative hearing, including, but not limited to, applicable
31 laws and regulations, enforcement procedures, due process,
32 evaluation of evidence, hearing procedures, and effective oral and
33 written communication. Upon the approval of the governing body
34 or chief executive officer of the issuing agency, up to 12 hours of
35 relevant experience may be substituted for up to 12 hours of
36 training. Up to eight hours of the training requirements described
37 in this subparagraph may be credited to an individual, at the
38 discretion of the governing body or chief executive officer of the
39 issuing agency, based upon training programs or courses described

1 in this subparagraph that the individual attended within the last
2 five years.

3 (5) The designated municipal employee who issues a notice of
4 violation shall not be required to participate in an administrative
5 hearing. The issuing agency shall not be required to produce any
6 evidence other than, in proper form, the notice of violation or copy
7 thereof, including the photograph, video, or other visual image of
8 the vehicle's license plate, and information received from the
9 Department of Motor Vehicles identifying the registered owner
10 of the vehicle. The documentation in proper form shall be prima
11 facie evidence of the violation.

12 (6) The examiner's final decision following the administrative
13 hearing may be personally delivered to the person by the examiner
14 or sent by first-class mail.

15 (7) Following a determination by the examiner that a person
16 has committed the violation, the examiner may, consistent with
17 the written guidelines established by the issuing agency, allow
18 payment of the civil penalty in installments, or an issuing agency
19 may allow for deferred payment or payments in installments, if
20 the person provides evidence satisfactory to the examiner or the
21 issuing agency, as the case may be, of an inability to pay the civil
22 penalty in full. If authorized by the governing body of the issuing
23 agency, the examiner may permit the performance of community
24 service in lieu of payment of the civil penalty.

25 (8) If a notice of violation is dismissed following an
26 administrative hearing, any civil penalty, if paid, shall be refunded
27 by the issuing agency within 30 days.

28 22428. (a) Within 30 days after personal delivery or mailing
29 of the final decision described in subdivision (c) of Section 22427,
30 the contestant may seek review by filing an appeal to the superior
31 court, where the case shall be heard de novo, except that the
32 contents of the processing agency's file in the case on appeal shall
33 be received in evidence. A copy of the notice of violation shall be
34 admitted into evidence as prima facie evidence of the facts stated
35 in the notice. A copy of the notice of appeal shall be served in
36 person or by first-class mail upon the processing agency by the
37 contestant. For purposes of computing the 30-day period, Section
38 1013 of the Code of Civil Procedure shall be applicable. A
39 proceeding under this subdivision is a limited civil case.

1 (b) The fee for filing the notice of appeal shall be as provided
2 in Section 70615 of the Government Code. The court shall request
3 that the issuing agency's file on the case be forwarded to the court,
4 to be received within 15 calendar days of the request. The court
5 shall notify the contestant of the appearance date by mail or
6 personal delivery. The court shall retain the fee under Section
7 70615 of the Government Code regardless of the outcome of the
8 appeal. If the appellant prevails, this fee and any payment of the
9 civil penalty shall be promptly refunded by the issuing agency in
10 accordance with the judgment of the court.

11 (c) The conduct of the hearing on appeal under this section is
12 a subordinate judicial duty that may be performed by a
13 commissioner or other subordinate judicial officer at the direction
14 of the presiding judge of the court.

15 (d) If a notice of appeal of the examiner's decision is not filed
16 within the period set forth in subdivision (a), the decision shall be
17 deemed final.

18 (e) If the civil penalty has not been paid and the decision is
19 adverse to the contestant, the processing agency may, promptly
20 after the decision becomes final, proceed to collect the civil penalty
21 under Section 22426.

22 22429. (a) A city or city and county shall offer a diversion
23 program for indigent speed safety system violation recipients, to
24 perform community service in lieu of paying the penalty for an
25 automated speed system violation.

26 (b) A city or city and county shall offer the ability for indigent
27 speed safety system violation recipients to pay applicable fines
28 and penalties over a period of time under a payment plan with
29 monthly installments of no more than twenty-five dollars (\$25)
30 and shall limit the processing fee to participate in a payment plan
31 to five dollars (\$5) or less.

32 (c) Notwithstanding subdivisions (a) and (b), a city or city and
33 county shall reduce the applicable fines and penalties by 80 percent
34 for indigent persons, and by 50 percent for individuals 200 percent
35 above the federal poverty level.

36 22430. A city or city and county shall each develop and submit
37 to their respective governing body a Speed Safety System Report,
38 two years after initial implementation of the program and at the
39 end of the pilot program that includes all of the following
40 information:

- 1 (a) A description of how the speed safety system was used.
- 2 (b) Whether and how often any system data was shared with
- 3 outside entities, the name of any recipient entity, the type or types
- 4 of data disclosed, and the legal reason for the disclosure.
- 5 (c) A summary of any community complaints or concerns about
- 6 the speed safety system.
- 7 (d) Results of any internal audits, information about any
- 8 violations of the Speed Safety System Use Policy, and any actions
- 9 taken in response.
- 10 (e) Information regarding the impact the speed safety system
- 11 has had on the streets where the speed safety system was deployed.
- 12 (f) A summary of any public record act requests.
- 13 (g) A list of system locations that did not meet the threshold for
- 14 continuance of a program pursuant to paragraph (1) of subdivision
- 15 (p) of Section 22425, and whether further traffic-calming measures
- 16 are in planning or construction, or there is a decision to halt
- 17 operation of the program in those locations.
- 18 22431. Any city or city and county that used speed safety
- 19 systems shall, on or before March 1 of the fifth year in which the
- 20 system has been implemented, submit to the transportation
- 21 committees of the Legislature an evaluation of the speed safety
- 22 system in their respective jurisdictions to determine the system's
- 23 impact on street safety and the system's economic impact on the
- 24 communities where the system is utilized. The report shall be made
- 25 available on the internet websites of the respective jurisdictions
- 26 and shall include all of the following information:
- 27 (a) Data, before and after implementation of the system, on the
- 28 number and proportion of vehicles speeding from 11 to 19 miles
- 29 per hour over the legal speed limit, inclusive, from 20 to 29 miles
- 30 per hour over the legal speed limit, inclusive, from 30 to 39 miles
- 31 per hour over the legal speed limit, inclusive, and every additional
- 32 ~~10 miles per hour~~ *10-miles-per-hour* increment thereafter on a
- 33 street or portion of a street in which ~~an~~ *a* system is used to enforce
- 34 speed limits. To the extent feasible, the data should be collected
- 35 at the same time of day, day of week, and location.
- 36 (b) The number of notices of violation issued under the program
- 37 by month and year, the corridors or locations where violations
- 38 occurred, and the number of vehicles with two or more violations
- 39 in a monthly period and a yearly period.

1 (c) Data, before and after implementation of the system, on the
2 number of traffic collisions that occurred where speed safety
3 systems are used, relative to citywide data, and the transportation
4 mode of the parties involved. The data on traffic collisions shall
5 be categorized by injury severity, such as property damage only,
6 complaint of pain, other visible injury, or severe or fatal injury.

7 (d) The number of violations paid, the number of delinquent
8 violations, and the number of violations for which an initial review
9 is requested. For the violations in which an initial review was
10 requested, the report shall indicate the number of violations that
11 went to initial review, administrative hearing, and de novo hearing,
12 the number of notices that were dismissed at each level of review,
13 and the number of notices that were not dismissed after each level
14 of review.

15 (e) The costs associated with implementation and operation of
16 the speed safety systems, and revenues collected by each
17 jurisdiction.

18 (f) A racial and economic equity impact analysis, developed in
19 collaboration with local racial justice and economic equity
20 stakeholder groups.

21 22432. This article shall remain in effect only until January
22 1, 2028, and as of that date is repealed.

23 ~~SEC. 7.~~

24 *SEC. 5.* The Legislature finds and declares that a special statute
25 is necessary and that a general statute cannot be made applicable
26 within the meaning of Section 16 of Article IV of the California
27 Constitution because of the unique circumstances with traffic speed
28 enforcement in the Cities of Los Angeles, Oakland, San Jose, ~~and~~
29 Glendale, ~~one southern California city,~~ and *Palm Springs*, and the
30 City and County of San Francisco.

31 ~~SEC. 8.~~

32 *SEC. 6.* The Legislature finds and declares that Section ~~6 4~~ of
33 this act, which adds Section 22425 to the Vehicle Code, imposes
34 a limitation on the public's right of access to the meetings of public
35 bodies or the writings of public officials and agencies within the
36 meaning of Section 3 of Article I of the California Constitution.
37 Pursuant to that constitutional provision, the Legislature makes
38 the following findings to demonstrate the interest protected by this
39 limitation and the need for protecting that interest:

1 To protect the privacy interests of persons who are issued notices
2 of violation under a speed safety systems pilot program, the
3 Legislature finds and declares that the photographic, video, or
4 other visual or administrative records generated by the program
5 shall be confidential, and shall be made available only to alleged
6 violators and to governmental agencies solely for the purpose of
7 enforcing these violations and assessing the impact of the use of
8 speed safety systems, as required by this act.

O

Date of Hearing: April 19, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION

Jesse Gabriel, Chair

AB 2336 (Friedman) – As Amended March 22, 2022

SUBJECT: Vehicles: Speed Safety System Pilot Program

SUMMARY: Establishes a five-year pilot program to give local transportation authorities in the Cities of San Jose, Oakland, Los Angeles, Glendale, one unspecified southern California city, and the City and County of San Francisco the authority to install speed safety systems.

Specifically, **this bill:**

- 1) Authorizes a five-year speed safety system pilot program, from 2023 to 2028, in San Jose, Oakland, Los Angeles, Glendale, one unspecified Southern California city, and San Francisco to enforce speed limits on no more than 15% of their streets in the following areas:
 - The streets with the highest injuries and fatalities in the jurisdiction, referred to as a safety corridor.
 - On a street a local authority has determined to have had a high number of incidents for motor vehicle speed contests or motor vehicle exhibitions of speed.
 - School zones.
- 2) Defines a “speed safety system” as a fixed or mobile radar or laser system or any other electronic device that utilizes automated equipment to detect a violation of speeding laws and is designed to obtain a clear photograph, video recording, or other visual image of a vehicle license plate and defines “automated speed violation” as a violation of a speed law detected by a speed safety system operated pursuant to this article.
- 3) Specifies that speed safety systems are not to be operated on any California state route, including all freeways and expressways, U. S. Highway, Interstate Highway or any public road in an unincorporated county where the Commissioner of the California Highway Patrol (CHP) has full responsibility and primary jurisdiction for the administration and enforcement of the laws, and for the investigation of traffic accidents.
- 4) Provides that a speed safety system shall not continue to operate on any given street if within the first 18 months of installation of a system, at least one of the following thresholds has not been met:
 - Percentage of automated speed violations decreased by at least 25%.
 - Percentage of violators who received two or more violations decreased by at least 50%.
- 5) Provides that the cameras may continue to operate if traffic calming measures are added to the street and authorizes the cameras to continue to be used for up to two years, with a vehicle speed feedback sign while traffic calming measures are being planned or constructed. If construction of traffic calming measures has not begun within two years, use of cameras

shall be halted. If violations do not decrease one year after traffic calming measures have been added, then a city or county shall either construct additional traffic-calming measures or cease operation of the system on that street.

- 6) Defines “traffic calming measure” to include, but not be limited to: bicycle lanes, chicanes, chokers, curb extensions, median islands, raised crosswalks, road diets, roundabouts, speed humps or speed tables, and traffic circles.
- 7) Permits the use of speed safety systems in school zones two hours before school and two hours after school where the posted speed limit is 30 mph or higher when children are not present.
- 8) Prohibits the use of mobile systems for the first two years of the pilot.
- 9) Provides that speed safety systems must:
 - Clearly identify the presence of the fixed or mobile speed safety system with signs stating “Photo Enforced,” along with the posted speed limit. The signs must be visible to traffic and posted at all locations, as determined by the California Department of Transportation (Caltrans) and the local California Traffic Control Devices Committee;
 - Identify vehicles containing a mobile speed safety system with distinctive markings, including information that the system is being operated for “Photo Enforcement” purposes, identify the streets or portions of streets that have been approved for speed safety systems, and post the locations and hours of enforcement on the municipality’s Internet website.
 - Use properly trained designated municipal employees, as specified, to operate the speed safety systems and make determinations on when notices of violation should be issued. Requires training and proof of successful completion of peace officer and municipal training to be retained by the pilot cities, as specified.
 - Ensure regular inspection and certification of the speed safety system to ensure proper calibration; conduct an annual inspection by independent calibration laboratory; and document the inspection, operation, and calibration of the speed safety system.
 - Use fixed and mobile speed safety systems that provide real-time notification when violations are detected.
- 10) Requires the pilot cities to meet numerous consumer protection and privacy conditions including:
 - Conduct a public information campaign for 30 days before deployment.
 - Only issue warning notices during the first 30 days of enforcement.
 - Prior to implementation, adopt a Speed Safety System Use Policy and a Speed Safety System Impact Report and work collaboratively with relevant local stakeholder

organizations, including racial equity, privacy protection, and economic justice groups to develop these.

- Include a clear photograph, video recording, or other visual image of the license plate and rear of the vehicle only, a citation of the law violated, the camera location, and the date and time when the violation occurred. Notices of violation must exclude images of the rear window area of the vehicle.
- Keep speed safety system data and records confidential, except as required by the Public Records Act. The pilot cities are permitted to retain speed safety system data and evidence for 60 days and speed safety system administrative records for 120 days following final disposition of a violation, but are required to destroy any speed safety system data within five days if the data shows no evidence of a speeding violation.
- Give the registered owner of the vehicle or an individual identified by the registered owner as the driver of the vehicle at the time of the alleged violation the right to review the photographic, video, or visual evidence of the alleged violation.
- Prohibits the use of facial recognition software.
- Require information collected and maintained using a speed safety system to be used only to administer a speed safety system program and prohibits disclosure to any other person, including a state or federal agency, except as required by law, court order or subpoena.
- Meet vendor contracting requirements, as specified, including a requirement that any speed safety system data collected is confidential and may not be shared, repurposed, or monetized for purposes other than speed safety system enforcement.
- Issue violations only for violation of speeding 11 miles per hour (mph) or more over the posted speed limit, that carry a civil penalty of \$50, \$100, \$200 or \$500, cannot be used to suspend or revoke a driver's license, and cannot be used to assess a point against the driver.
- Provides an appeals process, as specified, including a diversion program for indigent violators, as specified.
- Use revenues from the speed safety system to recover program costs, build traffic calming measures, with excess revenue after three years going to the state's Active Transportation Program (ATP).
- Submit a Speed Safety System Report to the Legislature after the fifth and final year of the pilot.
- Requires the pilot cities to reduce ticket fines and penalties by 80% for people with household incomes less than 125% of the Federal Poverty Level and for people who receive CalFresh benefits, Supplemental Security Income (SSI), or Medi-Cal benefits, and by 50% for those living 200% above the federal poverty line.

- 11) Authorizes cities to transfer to the registration of a vehicle the penalties for offenses detected by a speed safety system.

EXISTING LAW:

- 1) Establishes a “basic speed law” that prohibits a person from driving a vehicle at a speed greater than is reasonable or prudent given the weather, visibility, traffic, highway conditions, and in no event at a speed that endangers the safety of persons or property. (Veh. Code Sec. 22350 *et seq.*)
- 2) Authorizes the use of automated traffic enforcement systems (i.e., red light cameras) at railroad crossings and intersections to record violations of unlawful grade crossings and running of red lights. (Veh. Code Secs. 22451, 21455.5, and 40518.)
- 3) Requires a peace officer or “qualified employee” of a law enforcement agency to review the photograph taken by an automated traffic enforcement system and issue a citation, as appropriate. (Veh. Code Sec. 21455.5(c)(2)(F).)
- 4) Conditions the use of red light cameras on several requirements and procedures, as specified. (Veh. Code Sec. 21455.5 *et seq.*)
- 5) Defines “Safety Corridor” as the 20% of a local jurisdictions streets with the highest injuries and fatalities, with a definition to be determined by Caltrans in the next revision of the California Manual on Uniform Traffic Control Devices. (Veh. Code Sec. 22358.7(b)(1).)
- 6) Authorizes jurisdictions to lower speed limits in safety corridors by 5 mph from the existing speed limit established by an engineering and traffic survey. (Veh. Code Sec. 22358.7(a).)

FISCAL EFFECT: Unknown

COMMENTS:

- 1) **Purpose of this bill:** This bill seeks to reduce traffic fatalities by establishing a five-year pilot program authorizing specified cities to install speed safety systems. This bill is author sponsored.
- 2) **Author’s statement:** According to the author:

Since the 1980s communities around the world have been using speed safety systems to slow drivers down. These cameras have proven to be widely effective. A 2005 systematic review of 14 studies of speed safety systems in Canada, Europe, Australia, and New Zealand found crash reductions of 5 to 69%, injury reductions of 12 to 65%, and fatality reductions of 17 to 71% at speed safety system locations after program implementation. Speed safety systems are used in over 150 communities across the United States, and more recently became eligible for federal funding under the Bipartisan Infrastructure Investment and Jobs Act as part of a new nationwide goal to achieve zero traffic fatalities. It is finally time for California to join 16 other states and authorize the use of speed safety systems.”

- 3) **Background:** AB 2363 (Friedman, Ch. 650, Stats. 2018) established the Zero Traffic Fatality Task Force (Task Force) in order to develop policies to reduce traffic fatalities to zero in California. Per this legislation, the California State Transportation Agency (CalSTA) formed the 25-member Task Force on June 5, 2019. Members of the Task Force included representatives from the California Highway Patrol, the University of California and other academic institutions, Caltrans, the State Department of Public Health, local governments, bicycle safety organizations, statewide motorist service membership organizations, transportation advocacy organizations, and labor organizations.

In January 2020, CalSTA in conjunction with the Task Force, released the *CalSTA Report of Findings: AB 2363 Zero Traffic Fatalities Task Force*. The report includes 27 policy recommendations, and 16 findings recommendations that are broken into four categories: establishing speed limits, engineering, enforcement, and education. Last year the Legislature passed AB 43 (Friedman, Ch. 690, Stats. 2021), which enacted several of the recommendations of that task force to give cities more flexibility to lower speed limits, including on the highest injury streets. Based on those recommendations, this bill would authorize cameras to be placed on safety corridors, which AB 43 defined as 20% of local authorities' streets with the highest injuries

The City of Los Angeles writes in support of this bill:

Years of national research, the laws of physics and common sense all point to an established fact about street safety: the faster people drive, the more dangerous and deadly our roads become. Speed is the number one factor in crash severity. Nationwide, 112,580 people were killed in speeding-related incidents from 2005 to 2014. California is no exception: every year for the past five years, more than 1,000 Californians have died in speed-related traffic collisions. Tens of thousands more have been injured. These deaths and injuries are preventable.

Across the United States, numerous peer-reviewed studies have shown that speed detection systems reduce the number of severe and fatal collisions by as much as 58 percent. Despite an established history, California law currently prohibits the use of these systems. Studies have shown that speed is the leading factor when determining fault in fatal and severe collisions, yet existing efforts have not led to the reduction in speed and traffic violence needed to save lives and make communities safe. California must provide communities with the option to pilot this public safety tool in order to create the expectation of regular speed checking on the most dangerous streets, in school zones, and on streets with a history of speed racing and motor vehicle exhibitions of speed.

In order to make sure the cameras are placed in areas where they can effectively reduce speed and not in areas that would bring in the most revenue, this bill provides that if the number of violations has not decreased by 25% over the course of 18 months, or the number of second violations has decreased by 50%, then the cameras cannot be used in that location unless traffic calming measures are installed. Cities would have two years to build the traffic calming measures, and during those two years, a vehicle speed feedback sign must be used. Feedback signs have been shown to reduce speeds by 3-4 mph and reduce crashes by 7%. If the traffic calming measures are not constructed in two years, the cameras can no longer be used. If the calming measures are not effective at reducing violations within a year, then additional calming measures must be installed, or the localities must halt the use of the cameras.

The Western States Trucking Association, writing in opposition to this bill, argues:

While WSTA appreciates your efforts to improve the safety of the motoring public, AB 2336 is excessively overbroad for a “pilot program.” It authorizes an unnecessarily large number of speed cameras to enforce any speed law, either through a fixed or mobile speed camera, within the cities of Los Angeles, Oakland, San Jose, San Francisco, as well as two other unnamed cities. Such cameras would only be required to cease operations within 18 months if one of the following thresholds has not been met: 1) automated speed violations were decreased by at least 25%; or 2) violators who received two or more violations decreased by at least 50%. Nevertheless, such thresholds can be ignored entirely, and the speed cameras can continue to be used, if certain “traffic calming measures” are implemented – many of which, including adding bike lanes and raised crosswalks, are not true traffic calming measures.

Nonetheless, this bill has broad support from a number of municipalities and nonprofits. The National Safety Council (NSC), a nonprofit safety advocacy group, writes in support:

Automated enforcement technologies are a proven life-saving tool. According to a system analysis completed by the National Highway Traffic Safety Administration (NHTSA), automated enforcement is highly effective in slowing down drivers and saving lives on the roadways. Automated enforcement helps ensure people drive at posted speed limits, which reduces the severity and likelihood of crashes.

- 4) **Privacy protections included in bill:** The author has included a number of provisions in this bill to ensure that the privacy of drivers is protected in the communities authorized to use speed safety systems. For example, the bill requires that video, or other visual or administrative records generated by the speed safety system be confidential, and shall only be used to administer a program, and shall not be disclosed to any other persons, including any other state or federal government agency or official for any other purpose, except as required by state or federal law, or court order.

The pilot cities are only permitted to retain speed safety system data and evidence for 60 days and speed safety system administrative records for 120 days following final disposition of a violation, after which the data, evidence, and administrative records must be destroyed in a manner that maintains the confidentiality of any person included in the evidence. Cities are also required to destroy any speed safety system data within five days if the data shows no evidence of a speeding violation. Finally, the bill also ensures that any vendors are held to these same standards and provides that any speed safety system data collected is confidential and may not be shared, repurposed, or monetized for purposes other than speed safety system enforcement. The bill additionally prohibits the use of facial recognition software.

While appreciative of the author’s efforts to address some privacy concerns, a coalition of organizations including Safer Streets LA, ACLU California Action, Electronic Frontier Foundation, and the Teamsters, among others (hereinafter “Coalition”), oppose this bill and write:

Automated traffic enforcement systems, such as those authorized by this bill, also raise numerous privacy concerns. By encouraging the use of surveillance technologies, like automated license plate readers (ALPRs), for enforcement of speed limits, AB 2336

subjects Californians to increased surveillance and perpetuates the false notion that this surveillance benefits the communities that are surveilled. The need for enforcement of speed limits does not warrant the creation of a new mechanism for government collection of large amounts of data on Californians.

While we appreciate efforts to address some of the privacy concerns with the surveillance technology, the bill does not strike the appropriate balance between personal privacy and government transparency. For example, by making all information captured by the systems confidential, even administrative data about how many people are being ticketed and at what speeds, the bill ensures no data about the harmful impact of the program will ever be publicly available.

Regarding the contention that the confidentiality protections in the bill will prohibit appropriate oversight of the program, the author offers the following amendment which would provide that data about the number of violations issued and the speeds at which they were issued are not “administrative records” under the bill, and therefore do not have to be deleted within 120 days. In practice, this should allow a critical oversight function of the bill, removing speed safety systems from streets where the percentage of violators who received two or more violations decreased by at least 50%, as specified. It may also ensure that these de-identified data are available pursuant to the Public Records Act, thereby ensuring a higher level of government transparency.

Author’s amendment:

On page 12, line 16, after “impacts of the system.” add “***data about the number of violations issued and the speeds at which they were issued for is not considered administrative records for the purposes of this section.***”

- 5) **Equity considerations included in bill:** The cost of fines and fees associated with traffic and parking citations has steadily increased over the last few decades. After adding on fees to base fines, tickets can total hundreds of dollars. Add-on fees for minor offenses double or quadruple the original fine, and until recently California suspended driver’s licenses for failure to pay traffic fines or for failing to appear to court for a traffic infraction.

Recognizing the impact traffic fines and fees have had on countless Californians, this bill includes several provisions to protect against burdensome fines. First, the fines in this bill are significantly lower than existing fines for speeding tickets. Fines are \$50 for going 11-15 mph over the speed limit, \$100 for going 15-25 mph over the speed limit, and \$200 for going 25 mph over the speed limit. Individuals going 100 mph over the speed limit will face a \$500 fine. In contrast, under existing law driving 1-15 mph over the speed limit results in a \$238 ticket. Driving 16-25 mph over the speed limit results in a \$367 ticket. Driving 26 mph over the speed limit would result in a \$490 ticket. Driving 100 mph or greater is a \$900 ticket.

Despite the limitations on fines required by the bill, the Peace Officers’ Research Association of California writes in opposition:

Although the fine is no more than \$125, it is still a lot to low-income families and senior citizens. We have seen the amount charged for tickets escalate rapidly. When you consider the penalty assessment added onto most tickets, it is often burdensome.

Our research indicates that many cities around the country have used automated speed enforcement and ultimately removed it. Even San Jose, which AB 2336 includes, had it from 1997 to 2003, and it was discontinued over 18 years ago—leading us to believe this is more about revenue generation than actual safety.

Furthermore, law enforcement officers use discretion and provide drivers an opportunity to mitigate the violation. Verbal and written warnings are often given in place of a ticket. They assess the situation, and after a conversation with the driver, they decide if a verbal or written warning is a better course of action. Law enforcement exercises discretion; cameras do not.

In the same vein, the Coalition raises several due process concerns, including the absence of any requirement that a municipality show that the required signage was in place or that the speed safety system was operating correctly; no requirement of proof that a ticket was received; and the fact that the bill does not allow for any extensions for those who cannot afford the fine. The Coalition argues in opposition:

[A]nyone who misses a deadline or does not have the resources to pay the fines will not be able to register their vehicles. Drivers who need to use the vehicle to get to work, drop their child off at school, or other life necessities will continue to do so regardless of registration status, subjecting them to more stops and ticketing in a continual downward legal and economic spiral. Women of color, particularly Black and Latinx women, are especially likely to suffer under AB 2336 because they tend to bear the brunt of the cost of citations, regardless of whether they incurred the citations.

Heeding this concern, and attempting to strike the appropriate balance, the author offers the following amendment, which would remove the sections of the bill authorizing a lien to be placed on a vehicle for failure to pay for offenses detected by a speed safety system.

Author's amendment:

Strike Sections 4 and 5 from the bill.

In seeking to appropriately balance due process concerns with the safety goals of this bill, the author has also ensured that drivers will not face negligent operator points if they receive a speeding ticket from a speed safety system. Generally, speeding tickets result in negligent operator points. The point system is used by DMV to determine if a driver should be considered a negligent operator. DMV may suspend or revoke a person's driving privilege for being a negligent operator. Also, points increase an individual's insurance rates. In addition to lower fines when compared to a traditional speeding ticket, this bill requires diversion programs to be offered to indigent persons. In addition, fines must be reduced by 80% for indigent individuals, and by 50% for those 200% above the federal poverty line. Payment plans of \$25 a month must also be offered. Finally, tickets are limited to one per day per car.

The author has also considered the unequal enforcement of traffic violations against African Americans in California. AB 593 (Weber, Ch. 466, Stats. 2015), enacted the Racial and Identity and Profiling Act (RIPA) of 2015, which requires local agencies to annually report data to the Attorney General on all stops conducted by peace officers. Data from that report

shows that African Americans are disproportionately stopped by law enforcement, and were more likely to be searched or detained than their white counterparts.

Speed cameras have often been viewed by some as a potential solution to discriminatory stops. However, it is important to note that some of the most dangerous roads in California and in the United States are in minority communities. As a result of these dangerous roads, people of color are disproportionately effected by traffic collisions. According to NRSS, African Americans, Latinos and Native Americans pedestrians are more likely to be killed in a traffic collision. The requirement for traffic calming measures to be added to areas where speed cameras exist and fail to curb speed violations should also help make these roads safer.

Finally, this bill attempts to further address equity concerns regarding the enforcement of traffic laws by requiring organizations that represent minority communities to be involved in the placement of these cameras.

In support of this bill, Streets for All, an LA County-based nonprofit advocating for safe, sustainable, equitable transportation writes:

AB 2336 was designed with equity in mind. Unlike the red light program, which results in hefty \$500 fines, AB 2336 has significantly lower fines starting at \$50 for going 11 miles per hour (mph) over the speed limit. Cities will be required to reduce fines for those under the poverty line by 80% or offer community service. The bill also requires cities to reduce fines by 50% for individuals 200% above the federal poverty line. Cities will be required to spend the revenue on engineering safer streets, cannot shift existing expenditures to backfill the new revenue, and will have to send the money to the state Active Transportation Program if they do not invest in safety measures within three years.

- 6) **Additional Author amendments to address opposition concerns:** The author offers three additional amendments. First, the author would like to designate Palm Springs as the final city authorized to participate in the pilot. Second, in response to concerns that the bill would not provide residents with adequate notice or visibility regarding speed safety systems in school zones, the author offers an amendment to require flashing beacons on the school zone speed limit sign to indicate the times during which the school zone speed limit is enforced with a speed safety system, and clarifies that the cameras may be in use *up to* two hours before and after school.

Finally, the author extends the time warnings must be issued rather than notices of violation when speed safety systems are first installed from 30 to 60 days.

Author's amendments:

- 1) On page 22, line 22, strike "one southern California city" and insert "***Palm Springs***"
- 2) On page 9, line 21, after "safety system" insert "***up to***"

On page 9, line 22, after "session begins and" insert "***up to***"

On page 9, line 23, after "session concludes." insert "***For these school zones, flashing beacons activated by a time clock, or other automatic device, or manually***"

activated shall be installed on the school zone speed limit sign and active to indicate the times during which the school zone speed limit is enforced with a speed safety system.”

3) On page 10, lines 26 and 31, strike “30” and replace with “60”.

- 7) **Prior legislation:** AB 43 (Friedman, Ch. 690, Stats. 2021), grants the Caltrans and local authorities greater flexibility in setting speed limits based on recommendations the Zero Traffic Fatality Task Force (Task Force) made in January 2020.

AB 550 (Chiu, 2021) was substantially similar to this bill. That bill was held on suspense in Assembly Appropriations Committee.

SB 735 (Rubio, 2021) authorized the use of ASE cameras in school zones. That bill died in Senate Transportation Committee.

AB 2363 (Friedman, Ch. 650, Stats. 2018), created the Zero Traffic Fatalities Task Force.

AB 342 (Chiu, 2017) would have established a five-year pilot program to give local transportation authorities in the City of San Jose and the City and County of San Francisco the authority to install ASE systems in the two municipalities.

SB 1325 (Kuehl, 2008) would have authorized the City of Beverly Hills to deploy an ASE system. SB 1325 failed passage in the Senate Transportation and Housing Committee.

SB 1300 (Kuehl, 2006) was similar to SB 1325 (Kuehl, 2008). SB 1300 failed passage in the Senate Transportation and Housing Committee.

SB 466 (Kuehl, 2005) was similar to SB 1325 (Kuehl, 2008). SB 466 failed passage in the Senate Transportation and Housing Committee.

AB 1022 (Oropeza, Ch. 511, Stats. 2003), refined the red light camera provisions after a number of legal challenges arose concerning the operation of the automated systems. These changes clarified responsibility for operation and maintenance of the system by local authorities and private contractors, the involvement of law enforcement personnel in citation issuance, restrictions on compensation to vendors, and the required consideration of alternative methods of enforcement.

SB 1136 (Kopp, Ch. 54, Stats. 1998), authorized the use of automated enforcement systems at red lights indefinitely.

SB 833 (Kopp, Ch. 922, Stats. 1995), authorized a three-year demonstration period to test the use and effectiveness of such cameras to reduce the incidence of drivers running red lights at intersections.

SB 1802 (Rosenthal, Ch. 1216, Stats. 1994), authorized the use of red light cameras to record violations occurring at rail crossing signals and gates.

- 8) **Double referral:** This bill was referred to the Assembly Transportation Committee where it was heard on March 28, 2022 and passed out 12-0.

REGISTERED SUPPORT / OPPOSITION:

Support

Alameda County Transportation Commission
 Alameda; City of
 Association of Bay Area Governments (ABAG)
 Bay Area Council
 Berkeley; City of
 Beverly Hills; City of
 California Bicycle Coalition
 California Public Bank Alliance, Sf Public Bank Coalition, Walksf, Sf Bicycle Coalition, United Educators Sf
 City of Beverly Hills
 City of Concord
 City of Los Angeles
 City of Saratoga
 Conor Lynch Foundation
 Hayward; City of
 Marin County Bicycle Coalition
 Mayor of City & County of San Francisco London Breed
 Metropolitan Transportation Commission
 Move La, a Project of Community Partners
 National Safety Council
 Oakland; City of
 San Francisco Bay Area Families for Safe Streets
 San Francisco Bicycle Coalition
 San Francisco County Transportation Authority
 San Francisco Municipal Transportation Agency (SFMTA)
 San Jose; City of
 Social Families for Safe Streets
 Spur
 Street Racing Kills
 Streets are For Everyone (SAFE)
 Streets for All
 Tenderloin Community Benefit District
 The East Cut Community Benefit District
 The San Fernando Valley Young Democrats
 Vision Zero Network
 Walk San Francisco

Opposition

ACLU California Action
 California Conference Board of The Amalgamated Transit Union
 California Teamsters Public Affairs Council

Electronic Frontier Foundation
Lawyers Committee for Civil Rights of The San Francisco Bay Area
Peace Officers Research Association of California (PORAC)
Privacy Rights Clearinghouse
Safer Streets LA
Western States Trucking Association

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200

Resolution in Support of Assembly Bill 2336 (Friedman)

(Solely as to the potential privacy impact)

Whereas, the California legislature is presently considering Assembly Bill 2336 (Friedman) (hereafter “AB 2336”), which if enacted, would authorize a trial program for automated speed enforcement cameras; and

Whereas, the City of Oakland is one of the named cities that would participate in the AB 2336 program if enacted; and

Whereas, the Privacy Advisory Commission (hereafter “PAC”) has been asked by the City Council to weigh in on AB 2336 as to the potential privacy impact from such a program; and

Whereas, AB 2336 is still an active proposed bill and therefore subject to future amendments; and

Whereas, the PAC is unable to conduct a complete and thorough review of AB 2336 due to its status as proposed but not yet enacted legislation; and

Whereas, the PAC is unable to conduct a review and make any recommendations on a specific proposal as to AB 2336’s implementation as no such proposal has been submitted by OakDOT or any other department; and

Whereas, the California legislature considered a similar proposal (AB 550 (Chiu)) in 2021 but did not ultimately approve it; and

Whereas, many significant privacy improvements to AB 2336 have occurred due to the previous concerns raised in 2021 as to AB 550 (Chiu) and this year’s proposed AB 2336, including but not limited to a) shortened data retention periods which mitigates against data mining, profiling, and greater intrusiveness from the collection of multiple data points, b) greater public-facing reporting requirements, c) required public safety improvements necessary to continue the program and also to receive funding, mandatory halting of the use of cameras if certain metrics and milestones are not met, d) mandatory maintenance to improve accuracy and ensure technology calibration, e) mandatory public outreach and equipment signage, f) a robust appeal mechanism, g) prohibited disclosure or use of data for purposes other than speed enforcement, h) prohibition on the use of facial recognition technology, i) mandatory use policy and impact statements; and

Whereas, on April 19, 2022, the Assembly Privacy and Consumer Protection committee approved AB 2336 by a 10-1 vote; now therefore be it

Resolved, the PAC finds that that the text of the proposed AB 2336, as amended on April 21, 2022, has sufficient guardrails in place to adequately protect the privacy interests of Oaklanders should the bill become law; and

Further Resolved, the PAC is not endorsing or opposing AB 2336 as a whole due to its status as a proposal subject to future amendments which prohibits the PAC from completing a thorough review; and

Further Resolved, should AB 2336 be enacted into law, the PAC will engage with OakDOT and the public to review the impact statement and develop a robust use policy with sufficient guardrails to protect the civil liberties of Oaklanders.



OAKLAND POLICE DEPARTMENT

Alcohol Tobacco and Firearms (ATF)

2021 Annual Report

OPD ATF Taskforce

The OPD ATF Taskforce supports firearm related investigations. The firearm investigations are often associated with Crime Guns identified through the National Integrated Ballistic Information Network (NIBIN), unserialized firearms (Ghost Guns), Convicted Felons in possession of firearms and the tracing or tracking of firearms through E-Trace. The Taskforce also provides OPD CID with access to forensic resources to support investigations involving gun violence in Oakland. The Taskforce also provides resources to the OPD Crime Gun Intelligence Center (CGIC). OPD CGIC utilizes the National Integrated Ballistic Information Network (NIBIN), which provides crucial intelligence about firearms related crimes committed in Oakland and the San Francisco Bay Area. ATF Special Agents and OPD Taskforce Officer/s frequently respond to assist several Bay Area Law Enforcement Agencies and the Oakland Police Department to conduct investigations of individuals or groups who victimize Oakland residents. The Taskforce also supports the Ceasefire program in the adoption of State firearm cases involving repeated violent Felons identified through Ceasefire.

Staffing

1. **Number of full and part time OPD officers assigned to ATF Task Force:** One part-time Officer. One full-time NIBIN analyst is currently assigned to OPD to assist with analytical data related to NIBIN Investigations.
2. **Number of hours worked as ATF Task Force Officer:** Regular 40 hours per week. However, the current task force officer is often assigned to other OPD operations based on OPD needs and priorities and whether or not there are active investigations.
3. **Funding source for ATF Task Force Officer salary:** OPD Budget – funded by OPD General Purpose Fund. Overtime related to ATF OPD Taskforce investigations are funded by the ATF.

Other Resources Provided

1. **Communication equipment:** ATF handheld radio, cellular phone & laptop computer.
2. **Surveillance equipment:** ATF owns and installs utility pole cameras which are utilized in some cases. A court order w/ judicial approval is required prior to any installation.
3. **Clerical/administrative staff hours:** NIBIN Analyst: Regular 40 hours per week.
4. **Funding sources for all the above:** ATF Budget.

Cases

1. **Number of cases ATF Task Force Officer was assigned to:** Eleven – a breakdown of these cases provided below:
 - a) Oakland gang member arrested by Ceasefire units with a firearm following his presence at an Oakland shooting. ATF investigation into the suspect led to a federal search warrant at his residence in Las Vegas, NV where numerous firearms and evidence of firearms trafficking were recovered. Defendant has plead guilty in federal court.
 - b) Investigation into Oakland gang member trafficking firearms from Texas to Oakland. A federal search warrant at his residence in San Leandro, CA as well as seizure of packages sent by the suspect from Texas led to the recovery of firearms, ammunition, and promethazine syrup which may have been stolen from a pharmacy.
 - c) ATF agents traveled to Houston, TX to obtain a federal indictment for firearms possession on a suspect in an Oakland marijuana dispensary homicide.
 - d) Investigation into Oakland gang members suspected to be involved in OHAPD shooting resulting in the injury of a juvenile. Federal search warrant at one residence led to the recovery of multiple firearms. Defendant was charged in federal court, case pending. A second related subject was identified as being involved in a Livermore armed robbery as well as a Florida home invasion. State search warrants at an Oakland and Antioch residence resulted in evidence of the crimes. Defendant was arrested for PC211 and pending charges in Florida.
 - e) Federal adoption of CHP firearm case led to a federal charge against an Oakland gang member. ATF arrested the suspect at his residence in Antioch where he attempted to flee by ramming law enforcement vehicles and was arrested with a loaded firearm on his person.
 - f) Investigation into a gang related homicide in Oakland. One of the involved parties was identified as an Oakland gang member who returned fire during the incident. The defendant is pending federal charges.
 - g) ATF investigators assisted OPD homicide with the fire-bombing of a residence which resulted in the death of two people, including a juvenile. Investigation is ongoing.
 - h) ATF investigators are assisting CHP with a freeway shooting in Oakland resulting in the death of a juvenile. DNA recovered by ATF lab on fired cartridge cases indicates previously theorized San Francisco gang conflict. Investigation is ongoing.
 - i) ATF provided lab assistance for the shooting of retired OPD Captain. DNA recovered by ATF lab on fired cartridge cases matched to one of the suspects. Investigation by ATF in Reno, NV led to evidence of a second suspect with the registered owner of the vehicle used during the shooting.
 - j) ATF provided lab assistance for the shooting of a retired law enforcement officer in Oakland. Investigation is ongoing.
 - k) ATF agents are currently reviewing all OPD firearm arrests for possible federal prosecution.
2. **Number of “duty to warn” cases:** None
3. **General types of cases:** Firearms investigations, NIBIN/CGIC investigations and Federally adopted State firearm cases.
4. **Number of times the ATF asked OPD to perform/OPD declined to perform:** None.
 - a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Note: When criteria is met for federal charging, consideration is provided to ATF through task force or officer.

Operations

1. **Number of times use of undercover officers were approved:** 0
2. **Number of instances where OPD Task Force officer managed informants:** 0
3. **Number of cases involving informants that ATF Task Force Officer worked on:** All cases except adopted cases.
4. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD:** None.
 - a. **Number of such requests that were denied:** N/A
 - b. **Reason for denial:** N/A
5. **Whether ATF Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected:** No.

Training and Compliance

1. **Description of training given to ATF Task Force Officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the ATF Task Force follows all OPD policies and has received several trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officer has also reviewed all provisions of the ATF Task Force MOU.
2. **Date of last training update:** Continuous Professional Training, June 2021
3. **Frequency with which ATF Task Force Officer briefs OPD supervisor on cases:** Weekly

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** ~~there were zero reportable potential or actual violations of law or policy during the reporting period OPD will provide information on violations that are subject to release under California's Public Records Act (the "PRA"), Government Code section 6254. Release of any of violations not covered by the PRA, however, would violate California law (832.7), as there is only one officer assigned to this task force.~~
2. **Number of potential violations:** Same answer as above.
3. **Actions taken to address actual or potential violations:** The officer follows OPD policies. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform to State and Federal laws.
4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. Going forward, they will consult on a biannual basis. OPD will also consult with the Privacy Advisory Commission about any proposed changes.

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. Whether OPD Task Force Officer submits SARs to NCRIC: No
2. Whether OPD officer receives SAR information: No

Command Structure for OPD Task Force Officer

1. Reports to whom at ATF? Resident Agent in Charge (RAC) Tommy Ho.
2. Reports to whom at OPD? Sergeant Steve Valle and Lieutenant Robert Rosin.



OAKLAND POLICE DEPARTMENT

Drug Enforcement Agency (DEA) Task Force

2021 Annual Report

OPD DEA Taskforce

The DEA State and Local Task Force combines federal leverage and the specialists available to the DEA with state and local officers' investigative talents and detailed knowledge of their jurisdiction to lead drug law enforcement investigations. The DEA shares resources with state and local officers, thereby increasing the investigative possibilities available to all. Participation in DEA Task Forces also allows the DEA to pay for the overtime and investigative expenses of participating police agencies.

Staffing

1. **Number of full and part time Oakland Police Department (OPD officers assigned to DEA Task Force:** One full-time officer
2. **Number of hours worked as DEA Task Force Officer:** Regular 40 hours per week.
3. **Funding source for DEA Task Force Officer salary:** OPD Budget

Other Resources Provided

1. **Communication equipment:** OPD handheld radio, cellular phone
2. **Surveillance equipment:** GPS Tracker, Wiretap Intercept Equipment (always in possession and managed by DEA), None.
3. **Clerical/administrative staff hours:** None
4. **Funding sources for all the above:** OPD Budget

Cases

1. **Number of cases DEA Task Force Officer was assigned to:** – case detail breakdown:

The goal of the Taskforce is to conduct targeted investigations into specific drug trafficking organizations (DTO) and the individuals within the DTOs who are engaged in high level narcotics distribution and trafficking. By conducting these longer federal investigations, the Taskforce is able to ensure entire DTO's are dismantled. Confronting and weakening DTOs closes off specific avenues in which drugs flow into the community. The Taskforce focuses primarily on heroin, methamphetamine, fentanyl, and cocaine trafficking; the Taskforce does not conduct any marijuana investigations.

Below is a summary of the cases worked on in 2021:

Oakland RO TFG / BB-21-0016

This is an active investigation into the crystal methamphetamine and counterfeit fentanyl pill drug trafficking organization (DTO) operating in and around the Greater Bay Area. The organization was responsible for transporting and trafficking crystal methamphetamine and "M30" fentanyl pills from Mexico into the U.S. from the southern California port of entry. The Oakland Task Force Group to date has arrested seven targets, seized \$293,845 in drug proceeds, approximately 10,000 "M30" fentanyl pills, a half kilogram of cocaine, approximately 30 pounds of crystal methamphetamine, and three firearms.

The main target of this investigation was responsible for supplying multiple pound quantities to a distributor who was identified as a member of the violent West Bully 223 street gang, operating in the East Bay area. This investigation was able to thwart the continued growth of the West Bully 223 street gang into a major crystal methamphetamine distributor in the East Bay area. The investigation into other criminal associates and co-conspirators is ongoing.

Oakland RO TFG / BB-21-0056 /

On August 12, 2021, agents from the DEA Oakland Resident Office (ORO) High Intensity Drug Trafficking Area (HIDTA) Task Force Group (TFG), along with the Oakland Alcohol, Tobacco, Firearms, and Explosives (ATF), United States Postal Inspection Service (USPIS), Concord Police Department (CPD), OPD, and the Alameda County Sheriff's Office (ACSO), arrested three suspects. These suspects were part of a firearms trafficking organization that was responsible for distributing firearms to violent drug trafficking organizations and known gang members throughout the Bay Area as well as other parts of the United States. As a result of the takedown, agents seized machine guns, privately made firearms (PMFs), silencers, firearms classified as assault weapons/rifles under California State Law, approximately over a thousand rounds of ammunition, high-capacity magazines, unfinished firearm receivers/frames. In total 55 firearms were seized. During the investigation, law enforcement conducted multiple undercover buys resulting in the purchase of 13 firearms and 17 Glock conversion switches, collectively. The undercover purchases netted commercial factory firearms as well as privately made firearms (PMFs), commonly referred to as "ghost guns." In July of 2021, DEA ORO TFG and ATF, utilized an undercover agent to purchase "M30" fentanyl pills from REMBERT in Concord, CA. Agents later identified the source of supply for those pills, and the investigation into this suspect continues.

Oakland RO TFG/BB-21-0041 /Fentanyl Overdose Death Investigation

On December 5, 2020, the DEA Oakland Resident Office (ORO) Task Force Group (TFG), in partnership with the United States Attorney's Office (USAO), and their state and local partners, executed the federal arrest warrant of an individual involved in the distribution of fentanyl resulting in death.

This was a six-month long investigation into the Oxycodone and fentanyl drug trafficking activities of the individual. This was a multi-agency investigation. Throughout this investigation, DEA ORO TFG conducted numerous surveillances, interviews, and search warrants to arrest the individual involved. DEA ORO TFG investigators were

also able to utilize technology to identify the individual as the drug trafficker who provided the lethal fentanyl to the overdose victim. Through partnering with their state and local counterparts, DEA ORO TFG was able to link the individual to multiple fentanyl related overdoses. The individual's fatal drug trafficking activities has him facing a mandatory minimum sentence of twenty years in federal prison.

OAKLAND RO TFG/ BB-21-0030

In December of, 2020, the DEA Oakland RO TFG initiated an investigation into the drug trafficking activities of an identified suspect. DEA ORO TFG investigators corroborated intelligence derived from a confidential source (CS) that the suspect was a multi-pound methamphetamine trafficker with ties to Los Angeles and Mexican based drug traffickers. The CS was able to identify locations, vehicles, and methods of operation for the suspect's drug trafficking organization (DTO), which is based in Oakland, CA.

On February 26, 2021, DEA ORO TFG, investigators learned from their CS that the suspect would be traveling to southern California to gain more supply of methamphetamine. OAK-TF-1 investigators then coordinated with California Highway Patrol (CHP) to conduct a traffic stop of the suspect once the vehicle entered the Northern District of California. DEA ORO TFG investigators utilized physical and electronic surveillance on the suspect while on Interstate 5 and 580. Once the suspect entered Alameda County, CHP initiated the stop. As a result of the traffic, CHP discovered 133 pounds of crystal methamphetamine in the suspect's vehicle ready for immediate distribution. The suspect was arrested and charged with federal drug trafficking violations by the United States Attorney's Office (USAO) in the Northern District of California.

Oakland RO TFG / BB-21-0026

In late 2020, the FBI Contra Costa County Safe Streets Task Force (CCCSSTF), DEA RO TFG, and the Concord Police Department (CPD) initiated an Organized Crime Drug Enforcement Task Force (OCDEFT) investigation "Operation Snow Storm" into a Honduran Drug Trafficking Organization (DTO) that distributes large quantities of fentanyl throughout the San Francisco Bay Area. The investigation revealed that several criminal street gang members in Contra Costa County were getting supplied large quantities of fentanyl by the Honduran DTO. A CPD confidential informant identified a high-level member of the DTO. In February 2021, agents learned that the suspect was previously intercepted on a DEA Oakland RO Enforcement Group Title III (T-III) wiretap investigation. In mid-February, DEA ORO TFG, in conjunction with FBI CCCSSTF conducted a buy walk operation with the suspect and purchased approximately a quarter pound of fentanyl. As a result of the aforementioned purchase, law enforcement applied for and received authorization for a federal T-III on the suspect's telephone. During the interception period, law enforcement conducted surveillance and traffic enforcement stops on members of the DTO which resulted in four arrests and approximately one kilogram of fentanyl seized. On May 25, 2021, at the conclusion of the T-III interception period, law enforcement served search warrants at five locations. Approximately 19 kilograms of fentanyl, \$37,000 in US Currency, two handguns, and a rifle were seized during the search warrants. The suspect along with seven other criminal associates were arrested on federal drug charges.

Oakland RO TFG Airport Interdiction

Oakland RO TFG have been working in conjunction with the Alameda County Sheriff's Office, Oakland International Airport Insider Threat Task Force. Oakland International Airport is a transit point for drug trafficking and bulk cash smuggling. To date, Oakland RO TFG have seized approximately \$900,000 in bulk currency suspected to be drug proceeds or utilized to facilitate drug trafficking.

2. **Number of "duty to warn" cases:** None
3. **General types of cases:** Narcotics investigations and money laundering investigations
4. **Number of times the DEA asked OPD to perform/OPD declined to perform:** None
 - a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Operations

1. **Number of times OPD officers were involved in undercover investigations:** OPD personnel were assigned in plain clothes or undercover capacity to approximately six investigations.
2. **Number of instances where OPD Task Force officer managed informants:** OPD TFO has three active informants
3. **Number of informant-involved cases in which the OPD DEA Task Force Officer actively participated:** All
4. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD:** None
 - a. **Number of such requests that were denied:** N/A
 - b. **Reason for denial:** N/A
5. **Whether DEA Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected:** No

Training and Compliance

1. **Description of training given to DEA Task Force Officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the DEA Task Force follows all OPD policies and has received several police trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officer has also reviewed all provisions of the DEA Task Force MOU.
2. **Date of last training update:** Continuous professional training (CPT) in January, 2021
3. **Frequency with which DEA Task Force Officer briefs OPD supervisor on cases:** Weekly

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** ~~there were zero reportable potential or actual violations of law or policy during the reporting period OPD will provide information on violations that are subject to release under California's Public Records Act (the "PRA"), Government Code section 6254. Release of any of violations not covered by the PRA, however, would violate California law (832.7), as there is only one officer assigned to this task force.~~
2. **Number of potential violations:** Same answer as above.

3. **Actions taken to address actual or potential violations:** The officer follows OPD policies, except where DEA policies are more restrictive. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform with State and Federal laws. Going forward, OPD will consult with Office of the City Attorney on a biannual basis.
4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. OPD will also consult with the Privacy Advisory Commission about any proposed changes.

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. **Whether OPD Task Force Officer submits SARs to NCRIC:** No.
2. **Whether OPD officer receives SAR information:** No.

Command Structure for OPD Task Force Officer

1. **Reports to whom at DEA?** HIDTA Task Force Group Supervisor Marcelus Ross
2. **Reports to whom at OPD?** Sergeant Valle and Lieutenant Nowak



OAKLAND POLICE DEPARTMENT United States Marshals Service (USMS) 2021 Annual Report

OPD USMS Taskforce

The USMS is responsible for enforcing federal court orders and serves as the administrative custodian of all **federal** warrants until they are executed or dismissed. The USMS also manages warrant information, investigates fugitive matters and executes arrest warrants.

The U.S. Marshals have a long history of providing assistance and expertise to other law enforcement agencies in support of fugitive investigations. The USMS Task Forces does not conduct an independent investigation of possible criminal activity. The USMS only seeks to apprehend individuals with active arrest warrants issued for them related to crimes which have targeted local residents. These crimes include; murder, rape, child molestation, robberies, felony assaults and large scale fraud operations. USMS TFs work by leveraging local police intel as well as other data sources (e.g. database searches, open source social media inquiries, and interviews of associates/ and family members).

Staffing

1. **Number of full and part time OPD officers assigned to USMS Task Force:** One full-time officer.
2. **Number of hours worked as USMS Task Force Officer:** Regular 40 hours per week. However, the OPD officer sometimes is asked to assist with OPD operations. The work assignment of this officer is based on OPD needs and priorities and whether there are active investigations.
3. **Funding source for USMS Task Force Officer salary:** OPD General Purpose Fund Budget.

Other Resources Provided

Communication equipment: OPD/USMS radio, cellular phone, laptop.

1. **Surveillance equipment:** None.
2. **Clerical/administrative staff hours:** None.
3. **Funding sources for all the above:** USMS Funds

Cases

1. **Number of cases USMS Task Force Officer was assigned to:** 73; a breakdown of fugitive apprehensions by originating crime type is provided below.

Originating Crime Type Leading To Warrant	Amount
Homicide	28
Robbery	12
Assault	4
Weapons Charges	11
Burglary	3
Rape	4
Aiding Escapee	1
Molesting a Minor	0
Kidnapping	2
Other (e.g. Hit and Run, PAL*, Probation)	8
Total	73

*PAL=parolee at large

2. **Number of “duty to warn” cases:** None
3. **General types of cases:** Local, state, and federal criminal arrest warrants.
4. **Number of times USMS asked OPD to perform/OPD declined to perform:** None
 - a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Operations

1. **Number of times OPD officers were involved in undercover investigations:** None.
2. **Number of instances where OPD Task Force officer managed informants:** None.
3. **Number of informant-involved cases in which the OPD USMS Task Force Officer actively participated:** None.
4. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD:** None.
 - a. **Number of such requests that were denied:** N/A
 - b. **Reason for denial:** N/A
5. **Whether USMS Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected:** No.

Training and Compliance

1. **Description of training given to USMS Task Force Officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the USMS Fugitive Task Force follows all OPD policies and procedures, and has received several police trainings, including, but not limited to continued professional training, procedural justice training, and annual firearms training.
2. **Date of last training update:** June 2021 Continuous Professional Training.
3. **Frequency with which USMS Task Force Officer briefs OPD supervisor on cases:** Weekly.

Actual and Potential Violations of Local/State Law

~~1. **Number of actual violations:** here were zero reportable potential or actual violations of law or policy during the reporting period OPD will provide information on violations that are subject to release under California's Public Records Act (the "PRA"), Government Code section 6254. Release of any of violations not covered by the PRA, however, would violate California law (832.7), as there is only one officer assigned to this task force.~~

~~2.1. **Number of potential violations:** Same answer as above.~~

~~3.2. **Actions taken to address actual or potential violations:** The Task Force Officer follows OPD policies. USMS Task Force Supervisor meets with OPD VCOC supervisor and commander weekly. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform with State and Federal laws. Going forward OPD will consult with City Attorney on a biannual basis.~~

~~4.3. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. OPD will also consult with the Privacy Advisory Commission about any proposed changes.~~

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. **Whether OPD Task Force Officer submits SARs to NCRIC:** No.
2. **Whether OPD officer receives SAR information:** No.

Command Structure for OPD Task Force Officer

1. **Reports to whom at USMS?** U.S. Marshal Assistant Chief Inspector Gerry Gutierrez.
2. **Reports to whom at OPD?** Sergeant Steve Valle and Lieutenant Robert Rosin.



OAKLAND POLICE DEPARTMENT

Federal Bureau of Investigations (FBI)

Violent Crimes / Safe Streets Taskforce

2021 Annual Report

OPD FBI Violent Crimes Taskforce

The OPD FBI Violent Crimes Taskforce which falls under The FBI's Safe Streets initiative, is a collaborative effort to address violence crimes within our community. The task force pursues violent gangs through sustained, proactive, coordinated and intelligence led investigations to obtain prosecutions that will further public safety while reducing harm and law enforcement's footprint.

Staffing

1. **Number of full and part time OPD officers assigned to FBI Task Force:** Two full-time officers.
2. **Number of hours worked as FBI Task Force Officer:** Regular 40 hours per week. However, the current task force officer is often assigned to other OPD operations based on OPD needs and priorities and whether or not there are active investigations.
3. **Funding source for FBI Task Force Officer salary:** OPD Budget.

Other Resources Provided

1. **Communication equipment:** None.
2. **Surveillance equipment:** None.
3. **Clerical/administrative staff hours:** None.
4. **Funding sources for all the above:** OPD Budget.

Cases

1. **Number of cases FBI Task Force Officer was assigned to:** Eleven – a breakdown of these cases provided below:
 - a. Two of the cases are ongoing homicide and felony assault cases involving criminal street gangs in the City of Oakland, as well as other Bay Area cities.
 - b. There are nine additional ongoing homicide cases in which the FBI Evidence Response Team (ERT) has processed evidence in all of the cases. The cases are all still ongoing; therefore, more detailed information cannot be released currently.
2. **Number of “duty to warn” cases:** N/A
3. **General types of cases:** Homicides and Felony Assault cases involving suspects identified in violent gangs / groups.
4. **Number of times the FBI asked OPD to perform/OPD declined to perform:** None.

- a. Reason for OPD declination (e.g. insufficient resources, local/state law): N/A

Operations

1. Number of times OPD officers were involved in undercover investigations: Five
2. Number of instances where OPD Task Force officer managed informants: None.
3. Number of informant-involved cases in which the OPD FBI Task Force Officer actively participated: All cases except adopted cases.
4. Number of requests from outside agencies (e.g. ICE) for records or data of OPD: None.
 - a. Number of such requests that were denied: N/A
 - b. Reason for denial: N/A
5. Whether FBI Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected: No.

Training and Compliance

1. Description of training given to FBI Task Force Officer by OPD to ensure compliance with Oakland and California law: The OPD officer assigned to the FBI Task Force follows all OPD policies and has received several trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officer has also reviewed all provisions of the FBI Task Force MOU.
2. Date of last training update: June 2021
3. Frequency with which FBI Task Force Officer briefs OPD supervisor on cases: Weekly

Actual and Potential Violations of Local/State Law

1. Number of actual violations: ~~there were zero reportable potential or actual violations of law or policy during the reporting period. Release of any of this information would violate California law (832.7), as there are two OPD officers currently assigned to this task force.~~
2. Number of potential violations: Same answer as above.
3. Actions taken to address actual or potential violations: The officer follows OPD policies. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform to State and Federal laws.
4. Recommendations by OPD to address prevention of future violations: OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. Going forward, they will consult on a biannual basis. OPD will also consult with the Privacy Advisory Commission about any proposed changes.

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. Whether OPD Task Force Officer submits SARs to NCRIC: No.

2. **Whether OPD officer receives SAR information:** No.

Command Structure for OPD Task Force Officer

1. **Reports to whom at FBI?** Supervisory Agent in Charge (ASAC) Darin Heideman
2. **Reports to whom at OPD?** Lieutenant Frederick Shavies II



OAKLAND POLICE DEPARTMENT

FBI Child Exploitation Taskforce

2021 Annual Report

OPD FBI Child Exploitation Taskforce Mission:

The mission of the Child Exploitation and Human Trafficking Task Force (CEHTTF) is to provide a rapid, proactive, and intelligence-driven investigative response to the sexual victimization of children, other crimes against children, and human trafficking within the FBI's jurisdiction; to identify and rescue victims of child exploitation and human trafficking; to reduce the vulnerability of children and adults to sexual exploitation and abuse; to reduce the negative impact of domestic and international parental rights disputes; and to strengthen the capabilities of the FBI and federal, state, local, and international law enforcement through training, intelligence-sharing, technical support, and investigative assistance.

The taskforce follows the following goals and priorities:

1. To rescue victims of sex trafficking that are being exploited on both city streets and through internet crimes.
2. To arrest those individuals who are in violation of prostituted related offenses including 647(a), 647(b), 653.22, and 653.23 P.C, 266 PC, 236.1 PC.
3. To gather intelligence and possibly initiate/pursue investigations on cases involving Human Trafficking or other criminal acts.
4. To assist OPD/FBI investigators on any open/active criminal case. Utilize Federal, state and local resources to locate victims of Human Trafficking and Child Exploitation and look for opportunities to prosecute the subjects Federally.

The defined priority threats that are aligned with the mission of the CEHTTFs are:

1. Child Abductions (Non-Ransom and Ransom)
2. Production/Manufacturing of Child Pornography
3. Sextortion
4. Electronic Groups/Organizations/Enterprises for Profit
5. Travelers/Enticement
6. Traders/Distributors of Child Pornography
7. Interstate Transportation of a Minor with Intent that Minor Engage in Any Illegal Sexual Activity
8. Human Trafficking
9. Child Sex Trafficking
10. Adult Sex Trafficking
11. Forced Labor
12. Domestic Servitude
13. International Parental Kidnapping
14. Possessors of Child Pornography
15. Child Sex Tourism
16. Unlawful Flight to Avoid Prosecution – Parental Kidnapping

17. All other Crimes Against Children and Human Trafficking matters within the FBI's jurisdiction

Staffing

1. **Number of full and part time Oakland Police Department (OPD officers assigned to FBI Task Force:** All Part-Time: (1 Lieutenant, 1 Sergeant and 4 Officers work Part-time Overtime Juvenile Rescue and Internet Crimes Against Children Operations)
2. **Number of hours worked as FBI Task Force Officer:** Each part-time TFO works on average 8 hours a week
3. **Funding source for FBI Task Force Officer salary:** FBI

Other Resources Provided

1. **Communication equipment:** OPD handheld radio, cellular phone
2. **Surveillance equipment:** Cellebrite machine*, ~~GoPro camera~~
3. **Clerical/administrative staff hours:** None
4. **Clerical/administrative equipment:** laptop computers, hard drives, vehicle usage
5. **Funding sources for all the above:** OPD Budget funds all OPD personnel standard salary and benefits; the FBI in 2021 reimbursed OPD for overtime expenses worked by the federally-deputized OPD members.

* Cellebrite is used in some investigations where there is probable cause for a search warrant, unless the person in possession of a phone (for use of Cellebrite technology) provides verbal consent to search a phone.

Cases

1. **Number of cases FBI Task Force Officer was assigned to:** 12 separate cases; the taskforce conducted over 51 operations in the city of Oakland related to these cases. The results were the following:
 - a. One hundred and twenty-nine (129) female adults were arrested for solicitation of prostitution (647(a) and (b) PC, 653.22 PC). They were all offered resources by a combination of several non-profit sexual assault advocate agencies.
 - b. One hundred and eleven (111) male adults were arrested for solicitation of prostitution (647(a) and (b) PC, 653.22 PC). The Special Victim Section followed up with "Dear John" letters to applicable residences.
 - c. Twenty-two (22) female juveniles were rescued from Human trafficking. They were all provided resources by a combination of several non-profit sexual assault advocate agencies.
 - d. Fourteen (14) sex traffickers were arrested and charged with human trafficking (236.1, 266 PC) as a direct result of operations.
 - e. The OPD/FBI VICE/Child Exploitation Unit Task Force vetted hundreds of child pornography cyber tips in 2021. This resulted in over 100 search warrants. Five (5) subjects were arrested and prosecuted for Child Pornography (311.11 PC).
 - f. The OPD/FBI VICE/Child Exploitation Unit Task Force has provided unmarked vehicles for the use of human trafficking investigations and operations.
 - g. In December 2021, The OPD/FBI VICE/Child Exploitation Unit Task Force received a cyber tip regarding an active sexual assault that was documented in child pornography. The OPD/FBI VICE/Child Exploitation Unit Task Force quickly

executed a search warrant service which resulted in the following: the scene was located; child pornography was recovered, and the suspect was arrested and prosecuted. Federal case social workers were also on scene to provide resources to the victim and family members. (Oakland PD RD#21-056098).

- a. In April 2020, the OPD/FBI VICE/Child Exploitation Unit Task Force conducted an operation on a "call-out" establishment. Several hours of surveillance were conducted and search warrants were executed.
2. **Number of "duty to warn" cases:** None
3. **General types of cases:** Human Trafficking and Internet Crimes
4. **Number of times the FBI asked OPD to perform/OPD declined to perform:** None
 - a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Operations

1. **Number of times OPD officers were involved in undercover investigations:** 51
Operations that included undercover officers
2. **Number of instances where OPD Task Force officer managed informants:** None
3. **Number of informant-involved cases in which the OPD FBI Task Force Officer actively participated:** None
4. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD:** None
 - a. **Number of such requests that were denied:** N/A
 - b. **Reason for denial:** N/A
5. **Whether FBI Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected:** No

Training and Compliance

1. **Description of training given to FBI Task Force Officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the FBI Task Force follows all OPD policies and has received several police trainings, including but not limited to: Continual Professional Training (CPT), Procedural Justice Training and annual firearms training. OPD VICE/CEU Officers have attended collaborative FBI surveillance training and monthly Innocence Lost meetings. The officer has also reviewed all provisions of the FBI Task Force MOU.
2. **Date of last training update:** FBI taskforce training in January, 2021
3. **Frequency with which FBI Task Force Officer briefs OPD supervisor on cases:** Weekly

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** ~~there were zero reportable potential or actual violations of law or policy during the reporting period. Release of any of this information would violate California law (832.7), as there is only one OPD officer assigned to this task force.~~
2. **Number of potential violations:** Same answer as above.
3. **Actions taken to address actual or potential violations:** The officer follows OPD policies. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform to State and Federal laws.

4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. Going forward, they will consult on a biannual basis. OPD will also consult with the Privacy Advisory Commission about any proposed changes.

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. **Whether OPD Task Force Officer submits SARs to NCRIC:** No.
2. **Whether OPD officer receives SAR information:** No.

Command Structure for OPD Task Force Officer

1. **Reports to whom at FBI?** Resident Agent in Charge (RAC) Martha Parker
2. **Reports to whom at OPD?** Task Officer reports to Sergeant of the SVS/VICE unit, who is currently Sgt. Marcos Campos. Sergeant reports to the Lieutenant of Special Victims Section is Lt. Alan Yu.



OAKLAND POLICE DEPARTMENT

Secret Service

2021 Annual Report

OPD United States Secret Service (USSS) Agreement

OPD and the USSS formalized an agreement related to the USSS Bay Area Identify Theft Strike Force / Electronic Crimes Task Force ("Task Force"). The Memorandum of Understanding (MOU) was signed by both parties in 2009 and articulates rules for reimbursement of participating OPD officers when working on overtime on official Task Force investigations.

Staffing

1. **Number of full and part time OPD officers assigned to USSS Task Force:** One part time officer, who also assists in Criminal Investigations Division (CID) general Crimes.
2. **Number of hours worked as USSS Task Force Officer:** Currently the task force officer spends the majority of his time in the General Crimes office and works with the USSS to assist with active investigations as needed. The assigned officer also uses the USSS task force to assist with digital forensic searches including computers and cell phones.
3. **Funding source for USSS Task Force Officer salary:** OPD Budget – funded by OPD General Purpose Fund.

Other Resources Provided

1. **Communication equipment:** OPD handheld radio, cellular phone.
2. **Surveillance equipment:** Bluetooth skimming detection device. None.
3. **Clerical/administrative staff hours:** None.
4. **Funding sources for all the above:** OPD Budget.

Cases

1. **Number of cases USSS Task Force Officer was assigned to:** This past year the USSS assisted OPD with approximately ten cell phone searches for felony assault. They also assisted OPD with digital forensics related to ATM skimmers and video related to ATM skimmers. The USSS has provided OPD with equipment and training to recognize, detect and locate Bluetooth skimming devices. The USSS also provided OPD with equipment and training to complete cell phone searches.

Staff assigned to the taskforce have not as of 2021 used surveillance devices to detect Bluetooth skimmers.

2. **General types of cases:** Fraud and identity theft investigations
3. **Number of times the USSS asked OPD to perform/OPD declined to perform:** None.

- a. Reason for OPD declination (e.g. insufficient resources, local/state law): N/A

Operations

1. Number of times OPD officers were involved in undercover investigations: None
2. Number of instances where OPD Task Force officer managed informants: None.
3. Number of informant-involved cases in which the OPD USSS Task Force Officer actively participated: None
4. Number of requests from outside agencies (e.g. ICE) for records or data of OPD: None.
 - a. Number of such requests that were denied: N/A
 - b. Reason for denial: N/A
5. Whether USSS Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected: No.

Training and Compliance

1. Description of training given to USSS Task Force Officer by OPD to ensure compliance with Oakland and California law: The OPD officer assigned to the USSS Task Force follows all OPD policies and has received several trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officer has also reviewed all provisions of the USSS Task Force MOU.
2. Date of last training: Sep 2021CPT. Additional USSS Bluetooth skimming device training May 2021
3. Frequency with which USSS Task Force Officer briefs OPD supervisor on cases: Daily

Actual and Potential Violations of Local/State Law

- ~~1. Number of actual violations: there were zero reportable potential or actual violations of law or policy during the reporting period: OPD will provide information on violations that are subject to release under California's Public Records Act (the "PRA"), Government Code section 6254. Release of any of violations not covered by the PRA, however, would violate California law (832.7), as there is only one officer assigned to this task force.~~
- ~~2.1. Number of potential violations: Same answer as above.~~
- ~~3.2. Actions taken to address actual or potential violations: The officer follows OPD policies. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform to State and Federal laws.~~
- ~~4.3. Recommendations by OPD to address prevention of future violations: OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. Going forward, they will consult on a biannual basis. OPD will also consult with the Privacy Advisory Commission about any proposed changes.~~

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. Whether OPD Task Force Officer submits SARs to NCRIC: No.
2. Whether OPD officer receives SAR information: No.

Command Structure for OPD Task Force Officer

1. **Reports to whom at USSS?** Assistant to the Special Agent In Charge (ATSAIC)
Danielle Lopez
2. **Reports to whom at OPD?** Sergeant Alexis Nash and Lieutenant Brad Young

City of Oakland

Economic Development & Workforce Dept. Impact Report for Commercial Corridor Security Camera Grant Program

A. Description

Resolution No. 88717 C.M.S., as amended and adopted on June 24, 2021, appropriated \$150,000 to fund cameras in business corridors in Council District 6 and Council District 7.

Funds will be granted to one or two Intermediary organizations (Intermediary) with ties to the impacted areas, who will purchase security cameras to be granted to businesses (Recipients) to place on their private property along the identified commercial corridors. Since a data-driven approach is the best way to ensure cameras are not deployed in a discriminatory, viewpoint-based, or biased manner, the City will rely on OPD data to identify areas with the highest number of service calls for criminal activity to deploy the security cameras (see Section **C. Location**, below).

The terms of the program, including the requirements outlined in this Impact Report and in the accompanying Use Policy, will be defined in the agreement between the City and the Intermediary. The Intermediary will manage the agreements with individual business Recipients who will be placing security cameras on their private property.

B. Purpose

The program responds to the requests of business owners and residents in the identified areas by implementing a systematic approach to strengthen business corridors in East Oakland through a comprehensive security camera program. The purpose of this program is to support the revitalization of historically underinvested commercial corridors by increasing safety for residents, shoppers, employees, and small business owners. This is consistent with the Crime Prevention Through Environmental Design (CPTED) framework which works by decreasing the ability to commit a crime and increasing the chances that the crime will be seen and reported by naturally integrating security measures into the community with the goal of increasing quality of life, decreasing the fear of crime and decreasing crime.¹

The goals of the Security Camera Grant Program are twofold:

¹ <https://www.oaklandca.gov/resources/crime-prevention-through-environmental-design-cpted>

First, the presence of quality security cameras demonstrates to these majority-Black and Latinx small business communities in East Oakland the City's commitment to their safety and security and the City's investment in the community. This investment will enhance a culture of safety and security in the neighborhoods and along vital commercial corridors in East Oakland. There will be an immediate mitigating effect on illegal activity because security cameras will serve as a visual deterrent to potential criminal activity.

Second, installing security cameras assists in deterring crime and promotes overall crime prevention in commercial corridors. The Intermediary will register the security cameras with OPD's existing Register Your Security Camera program.² The cameras may capture video evidence that produces supporting information needed to build credible cases for prosecution. Over time, the video evidence may lead to a notable increase in prosecutions and convictions.

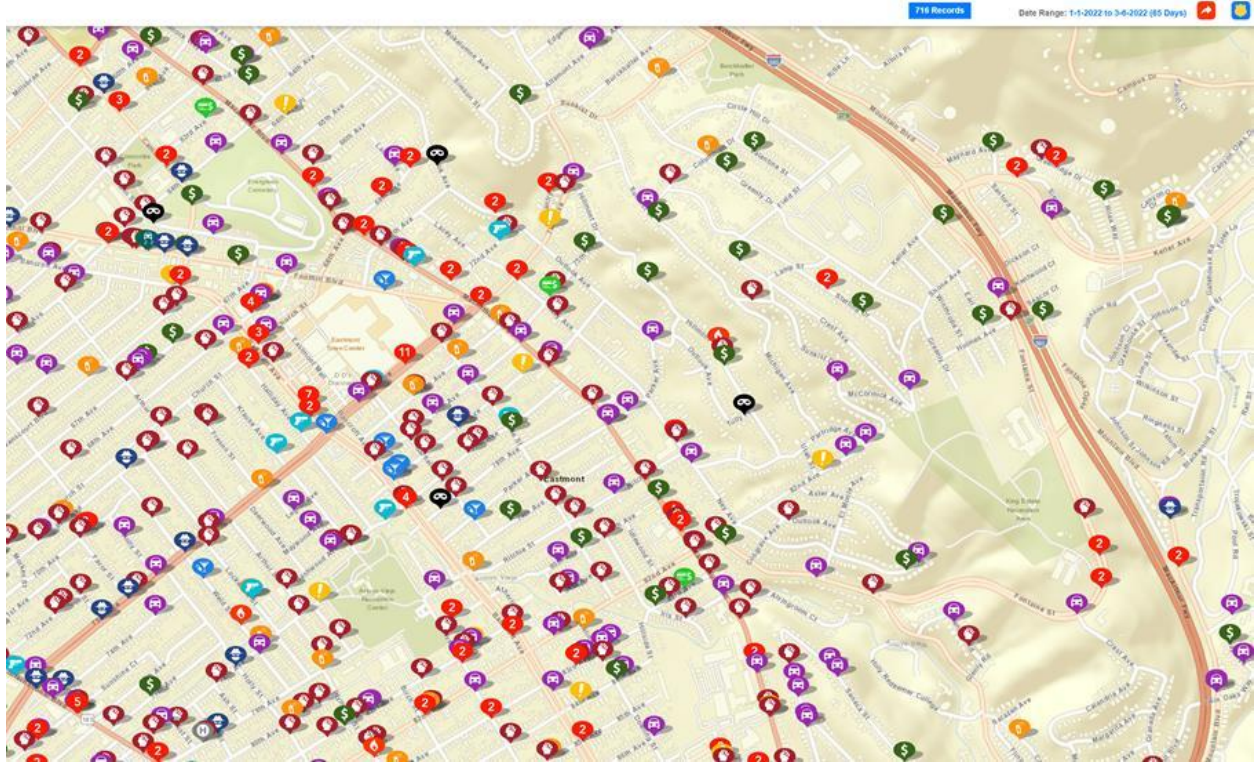
C. Location

The grants will be issued to place cameras at strategic locations on private property on the premises of businesses in East Oakland. The identification of the priority areas for Program eligibility, including at least 3-4 areas in Districts 6 and 7, will be determined by crime levels and other public safety indicators, including areas where criminal activity has increased in the past several years during the COVID-19 pandemic. Preliminary analysis of available data shows that the following 4 Commercial Corridors in Council Districts 6 and 7 are likely to be a focus for the Program:

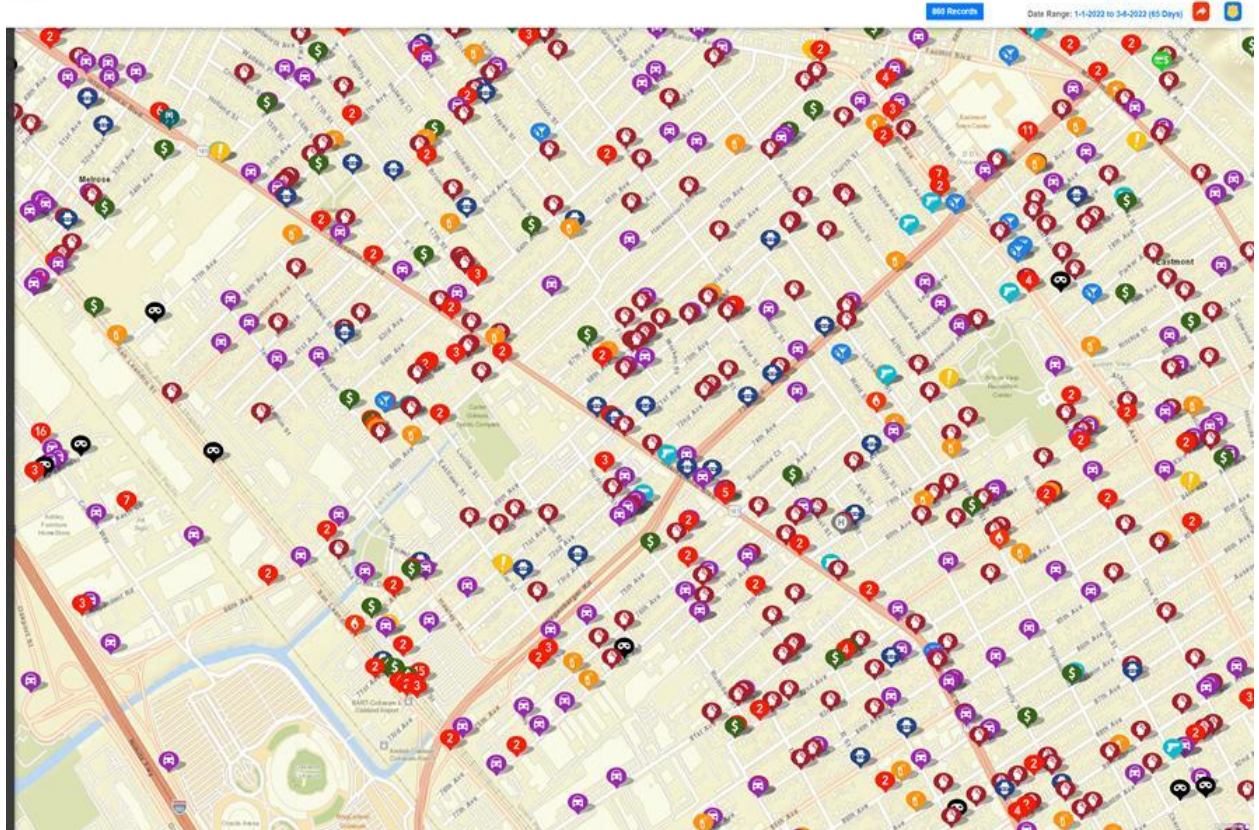
1. Eastmont Business Corridor (Foothill Ave/ MacArthur Blvd, 73rd-77th Ave)
2. Havenscourt Business Corridor (Bancroft, 64th – 67th Ave)
3. Hegenberger Rd (between Doolittle Dr and International Blvd)
4. Foothill Square

The following maps show the number of service calls related to the reported acts of criminal activity in those specified areas. These maps underscore the vital need for a security camera system in these areas. This data is derived from service calls to OPD over a recent 60-day period.

² <https://www.oaklandca.gov/services/register-your-security-camera>



716 Records Date Range: 1-1-2022 to 3-4-2022 (85 Days) RECEIVE ALERTS



In October 2021, EWDD staff reviewed data by Police Beat (see **Attachment A**) and calculated the percentage change in crime reported between FY 2019-20 and FY 2020-21. While several Police Beats that include commercial corridors experienced double digit drops in reported crime, others saw increases. Of the 57 Police Beats across Oakland, 38 saw a reduction in crime reported. The 19 Police Beats that saw an increase in reported crime are concentrated in Central East Oakland and Deep East Oakland, including in the commercial districts identified above. Some of those commercial areas that saw double-digit increases in crime are shown in **Table 1**, below:

Table 1: Police Beat Change in Reported Crime FY 2019-20 and FY 2020-21

Police Beat	FY 2019-20	FY 2020-21	% Change
13Z-Montclair/Piedmont Pines/Central Hills	402	417	3.73%
16X-Lakeshore Ave./Trestle Glen/Crocker Highlands	167	175	4.79%
20X-Jingletown/part of Fruitvale District	811	871	7.40%
21Y-Upper Fruitvale	530	551	3.96%
27X-Fairfax	482	532	10.37%
27Y-Seminary	551	711	29.04%
30x-Havenscourt/ Arroyo Viejo	735	865	17.69%
34X-Elmhurst	615	730	18.70%

Focusing these resources along these identified corridors addresses longstanding racial disparities in access to City resources in neighborhoods with significant Black and Latinx and lower-income populations. For example, the 4 identified commercial corridors above are in census tracts with the following racial and income statistics, according to the OakDot Equity Toolbox:³

1. Eastmont - 97% People of Color (POC); 53% Low Income
2. Havenscourt - 92% POC; 45% Low Income
3. Hegenberger– 98% POC; 52% Low Income
4. Foothill Square - 88% POC; 40% Low Income

D. Impact

EWDD recognizes that all people have an inalienable right to privacy and are committed to protecting and safeguarding this right.

The proposed Security Camera Program does not seek to track movement of individuals. Nevertheless, EWDD recognizes that the public may be concerned that allocating City funds to place security cameras in public areas could capture information about individuals that could

³ <https://www.oaklandca.gov/resources/oakdot-geographic-equity-toolbox>

potentially be used to track an individual's movement or be abused for other inappropriate purposes, including in the following specific areas:

- **Identity capture.** The public may be concerned that the cameras will capture personally identifiable information without notice or consent. Although the security cameras will be placed in private businesses where individuals do not have a reasonable expectation of privacy, and the data will only be made available to the City upon request for investigation of specific incidences involving suspected criminal activity or illegal dumping, camera footage may capture information about vehicle occupants, and/or license plate information that could be used to determine the registered owner. In addition, vehicle occupants or immediate surroundings (including addresses) may be pictured. As a result, it is possible that individuals with access to this data could do additional research to identify the individual.
- **Misidentification.** The public may be concerned that individuals may be misidentified as the person driving a vehicle and is committing a crime or engaging in illegal dumping. This could lead to government actions against such individuals in error.
- **Activity monitoring.** The public may be concerned that the cameras' data will enable individuals' behaviors to be revealed to and/or monitored by the City, their partners or affiliates, companies interested in targeted marketing, and/or the public. Such concerns may include basic information about when individuals are in certain locations, as well as concerns about what government or individuals may infer from this data (i.e., marital fidelity, religious observance, or political activity). Although video recordings and license plate numbers are gathered from public places, this could conflict with an individual's expectation of locational privacy.

E. Mitigations

To avoid the collection of large amounts of security footage by the City, these cameras will be purchased by the Intermediary who will grant the cameras to private business Recipients who will monitor the footage. Recipients will enter into agreements with the Intermediary, and the data collected by Recipients will not be considered public record. Footage will only be shared with OPD in the investigation of a crime or by OPW in the investigation of illegal dumping, pursuant to the guidelines of the existing Security Camera Registry and Illegal Dumping Surveillance programs.

The cameras will be purchased by the Intermediary and granted to Recipient Businesses to place on their business premises to monitor activity in areas in which the public does not have a reasonable expectation of privacy to reduce criminal activity. The cameras shall not be used for monitoring any residences. If the Camera is equipped with a "zooming" feature, such

feature shall be disabled and remain unused by Recipient. The Agreements between the Intermediary and the Recipients will outline the requirements contained in this report. No security camera purchased through this program will have any type of facial recognition technology imbedded within them

If the business vacates or moves from that location, Recipient shall inform the Intermediary of their intent to vacate or move from the location. The Intermediary reserves the right upon being informed of such intent to remove the security camera and equipment as necessary.

The data will be accessed only by the Recipient. No data will be stored with the City other than data requested by OPD in the investigation of a crime or by OPW in the investigation of illegal dumping, pursuant to the guidelines of the existing Security Camera Registry and Illegal Dumping Surveillance programs.

F. Data Types and Sources

- 1) Image, video recordings
- 2) License plate information as visible in video recordings
- 3) Annual Report*

*Since the intent of this program is to provide funds to the Intermediary to provide cameras for Recipient businesses, any auditing or reporting requirements will be addressed in the Annual Report submitted by the City to the PAC, per the requirements defined in the Use Policy.

G. Data Security

- 1) Data Collection
 - i. The data from the cameras will not be collected or maintained by the City.
 - ii. Signs will be placed in the locations where cameras are installed advising people that the area is under video surveillance.
- 2) Data Access
 - i. Data will only made available upon request to OPD or OPW for the purposes of investigating reported crimes or illegal dumping, following the protocols of the existing City Camera Registry Program and OPW Illegal Dumping Surveillance Program.
 - ii. The OPD Camera Registry Program allows residents and business owners to register the locations of their video security systems with OPD. OPD will then be able to see where cameras are located. If a Recipient registers a camera, OPD will contact them if video footage is sought in connection to a criminal investigation.

- iii. Refer to OPW Illegal Dumping Surveillance Program guidelines for details on that program.
- 3) Data Protection
 - i. Since the data will not be collected or maintained by the City, there should be no data protection concerns.
- 4) Data Retention
 - i. Since the data will not be collected or maintained by the City, there should be no data retention concerns.
- 5) Public Access
 - i. Except where prohibited or limited by law, the public may access the City's video data through public records requests. However, prior to the release of any information to a security-related public records request, staff will consult with the City Attorney's Office for review and guidance.
- 6) Third-Party Data Sharing
 - i. There is no third-party data sharing associated with this proposed Program.

H. Fiscal Cost

\$150,000 was allocated in the FY 2021-2023 Biennial Budget to fund the Program. The fiscal costs for the Program include a grant to an Intermediary for the purchase of security cameras to be granted to and installed on the premises at Recipient businesses, plus any administrative costs to the Intermediary for administering the Program. Estimates obtained by EWD Staff for cost of the Security Camera itself have ranged from \$150 for the basic security camera to \$450 for the most sophisticated and versatile types of security equipment. The average cost of a security system and installation is \$1,327, or between \$617 and \$2,039. A security service adds to installation complexities but provides 24-hour monitoring and other upgrades at a monthly fee. The cost of the monitoring has been estimated from \$175 to \$400 per month based upon the frequency and level of reporting desired.

I. Third Party Dependence:

There is no third-party dependence associated with the Program as proposed.

J. Alternatives:

Status Quo - Do not deploy the security camera program. The funds authorized by Council in the Biennial budget will not be spent to implement the program, and the program will not be realized. Criminal activity in the targeted commercial districts identified above could continue to increase, with no specific resources or economic development strategy to address public safety concerns in these commercial areas.

City Ownership and Installation of Security Cameras – Rather than work through an Intermediary, the City could purchase, own, and install the cameras on private property. This

approach would require the City to execute multiple grant agreements with individual small businesses, many of whom may be unable or unwilling to meet the City's contracting requirements, which could create a barrier to accessing the Program which may exacerbate rather than improve existing disparities. In addition, City control and monitoring of security camera footage would require significant City resources beyond the funds allocated for this program and City control and collection of data would raise additional privacy concerns requiring extensive mitigation measures.

K. Track Record:

As stated above, the City already has a Camera Registry Program that is a map-based database and a website. The Registry allows residents and business owners to register the locations of their video security systems with OPD. OPD will then be able to see where cameras are located. If a Recipient registers a camera, OPD will contact them if video footage is sought in connection to a criminal investigation. This Program would provide funding to commercial areas in East Oakland to close racial disparities in funding access to purchase costly security equipment so that more small businesses in majority Black and Latinx communities can participate in and realize the benefits of the existing City Camera Registry program. The City will continue to track and analyze crime and illegal dumping data along these commercial corridors pre- and post- camera to measure outcomes.

The City of Rancho Palos Verdes offers a similar Public Safety Reimbursement Program to allow neighborhoods and individuals to purchase public safety equipment such as security cameras. Rancho Palo Verdes provides a one-time reimbursement for half of the cost of a new public safety purchase, up to \$2,000 for neighborhoods, and up to \$100 for individuals and waives permit fees directly related to the installation of the approved purchase.⁴ Philadelphia and Washington DC also offer similar programs.⁵

⁴ <https://www.rpvca.gov/1329/Public-Safety-Reimbursement-Program>

⁵ <https://www.phila.gov/programs/business-security-camera-program/>; <https://ovsig.dc.gov/service/private-security-camera-system-incentive-program>

City of Oakland

**Economic Development & Workforce Dept. Use Policy for
Commercial Corridor Security Camera Grant Program**

April 7, 2022

A. Purpose

Resolution No. 88717 C.M.S., as amended and adopted on June 24, 2021, appropriated \$150,000 to fund cameras in business corridors in Council District 6 and Council District 7.

Funds will be granted to one or two Intermediary organizations (Intermediary) with ties to the impacted areas, who will purchase security cameras to be granted to businesses (Recipients) to place on their private property along the identified commercial corridors. The City will rely on OPD data to identify areas with the highest number of service calls for criminal activity to deploy the security cameras.

The program responds to the requests of business owners and residents in the identified areas by implementing a systematic approach to strengthen business corridors in East Oakland communities through a comprehensive security camera program. The purpose of this program is to support the revitalization of historically underinvested commercial corridors by increasing safety for residents, shoppers, employees, and small business owners. The program goals are twofold:

First, the presence of quality security cameras demonstrates to our majority-Black and Latinx small business community in East Oakland the City's commitment to their safety and security and the City's investment in the community. Staff also believes there will be an immediate mitigating effect on illegal activity because security cameras will serve as a visual deterrent to potential criminal activity.

Second, installing security cameras not only assists in deterring crime but promotes overall crime prevention in our commercial corridors. Grant recipients will be strongly encouraged or required to register the security cameras with OPD's existing Register Your Security Camera program.¹ The cameras may capture video evidence that produces supporting information needed to build credible cases for prosecution. Over time, the video evidence may lead to a notable increase in prosecutions and convictions.

¹ <https://www.oaklandca.gov/services/register-your-security-camera>

B. Authorized Use

The cameras will be purchased by the Intermediary and granted to businesses Recipients to place on business premises (private property) along the identified commercial corridors to monitor activity in areas in which the public does not have a reasonable expectation of privacy to reduce criminal activity.

C. Data Collection

The data from the cameras will not be collected or maintained by the City. The only data that the City would have access to would be data collected upon request as evidence by OPD or OPW, which significantly limits the total amount of data available.

D. Data Access

Data will only made available upon request to OPD and OPW for the purposes of investigating reported crimes and/or illegal dumping, following the protocols of the existing OPD City Camera Registry Program and OPW Illegal Dumping Surveillance Program. The Camera Registry Program allows residents and business owners to register the locations of their video security systems with OPD. OPD will then be able to see where cameras are located. If a Recipient registers a camera, OPD will contact them if video footage is sought in connection to a criminal investigation.

E. Data Protection

Since the data will not be collected or maintained by the City, there should be no data protection concerns.

F. Data Retention

Since the data will not be collected or maintained by the City, there should be no data retention concerns.

G. Public Access

The only data that the City would have would be data collected upon request as evidence by OPD or OPW, which significantly limits the total amount of data available. Except where prohibited or limited by law, the public may access the City's video data through public records requests. However, prior to the release of any information to a surveillance-related public records request, staff will consult with the City Attorney's Office for review and guidance.

H. Third Party Data Sharing

There is no third-party data sharing associated with this proposed Program.

I. Training

The Intermediary and their staff who administer the Program will be trained on the City's Surveillance Technology Ordinance and Privacy Principals. The Intermediary will be bound, through the terms of their grant agreement with the City, to abide by the ordinance or face non-payment of funds under the contract.

J. Auditing and Oversight

The Economic and Workforce Development Department (EWDD) of the City will monitor performance of the Intermediary grantee to ensure compliance with the terms of the grant agreement. The Grant Agreement will include a requirement for a written Annual Surveillance Report concerning the grant funded Camera program. See **Attachment B** for a draft Grant Agreement between the City and the Intermediary.

The Intermediary organization will in turn manage the grants to individual business Recipients including compliance with the Program terms through a separate agreement between the Intermediary and each Recipient.

K. Maintenance

The security cameras and related equipment purchased with funds under this Program will be the property of the Recipient businesses. Any maintenance needs associated with the use of the security cameras or associated equipment will be the responsibility of the Recipient business.

ATTACHMENT B

OPD Crime Data by Police Beat

	FY19-20	FY20-21	% Change	FY21-22*
01X - Jack London Warehouse & Waterfront District	1,382	978	-29.23%	318
02X - Jack London Gateway to Mandela Pkwy	483	412	-14.70%	90
02Y - Prescott	473	358	-24.31%	57
03X - Chinatown to Lake Merritt Channel	938	564	-39.87%	138
03Y - Old Oakland to City Center	656	457	-30.34%	97
04X - Uptown & Lakeside	1,856	1,209	-34.86%	455
05X - Greater DeFremery	346	308	-10.98%	54
05Y - Port & former Oakland Army Base	211	162	-23.22%	30
06X - Durant Hoover	601	459	-23.63%	85
07X - McClymonds/Poplar/Clawson	658	657	-0.15%	113
08X - KONO to Harrison	1,938	1,335	-31.11%	396
09X - Piedmont Ave.	901	529	-41.29%	114
10X - Golden Gate	279	245	-12.19%	43
10Y - Longfellow & Santa Fe	314	274	-12.74%	58
11X - Idora Park & Fairview Park	340	235	-30.88%	47
12X - Temescal	1,094	428	-60.88%	151
12Y - Rockridge	988	383	-61.23%	130
13X - Upper Rockridge	165	165	0.00%	36
13Y - Hiller Highlands & North Hills	210	192	-8.57%	41
13Z - Montclair/Piedmont Pines/Central Hills	402	417	3.73%	95
14X - Adams Point	748	559	-25.27%	132
14Y - Upper Grand Ave.	663	429	-35.29%	122
15X - Peralta Heights & Haddon Hill	589	513	-12.90%	88
16X - Lakeshore Ave./Trestle Glen/Crocker Highlands	167	175	4.79%	25
16Y - Glenview	300	251	-16.33%	65
17X - Clinton Park	410	344	-16.10%	77
17Y - Bella Vista & Highland	398	395	-0.75%	76
18X - San Antonio Park	215	260	20.93%	61
18Y -	303	259	-14.52%	46
19X - EastLake/Embarcadero Cove/International Blvd. from Lake to 23rd Ave.	1,565	1,364	-12.84%	257
20X - Jingletown/part of Fruitvale	811	871	7.40%	159
21X - 23rd Ave./Central Reservoir	363	378	4.13%	61
21Y - Upper Fruitvale	530	551	3.96%	109
22X - Dimond/Oakmore/Lincoln Highlands	590	396	-32.88%	80
22Y - Woodminster/Redwood Heights/Cretmont/Bret Harte	529	549	3.78%	0
23X - part of Fruitvale	879	870	-1.02%	192
24X -	406	416	2.46%	78
24Y - Allendale	363	342	-5.79%	65

25X - Beulah Heights/Leona Heights/Laurel District	690	562	-18.55%	125
25Y - Merritt College/Skyline	165	116	-29.70%	27
26X - Melrose/Oakport/Coliseum Way	645	644	-0.16%	128
26Y - Lockwood	866	875	1.04%	170
27X - Fairfax	482	532	10.37%	85
27Y - Seminary	551	711	29.04%	160
28X - Maxwell Park	321	356	10.90%	54
29X - Picardy/Millsmont	667	643	-3.60%	129
30X - Havenscourt/Arroyo Viejo	735	865	17.69%	141
30Y - Eastmont/Eastmont Hills	643	619	-3.73%	118
31X - Coliseum/Airport/Airport Business Park	995	380	-61.81%	216
31Y - Brookfield Village/Columbian Gardens	927	731	-21.14%	175
31Z - Sobrante Park	283	316	11.66%	45
32X - Stonehurst/Durant Square	595	555	-6.72%	116
32Y - Los Palmas/Toler Heights	636	638	0.31%	151
33X - Woodland	721	799	10.82%	138
34X - Elmhurst	615	730	18.70%	125
35X - Kings Estate/Oak Knoll	597	627	5.03%	99
35Y - Sequoyah Heights/Elysian Fields/Chabot Park/Sheffield Village	286	306	6.99%	49

99X and 77X are used when an officer doesn't assign a beat

77X	1,169	738	-36.87%	176
99X	130	112	-13.85%	14

*partial year = July 1, 2021 to Sept. 15, 2021

**GRANT AGREEMENT
BETWEEN THE CITY OF OAKLAND
AND [TBD Intermediary Organization]**

This Grant Agreement (the “Agreement”) dated July ___, 2022 is made and entered into by and between the City of Oakland, a municipal corporation (the “City”), and the [TBD Intermediary Organization] (“Grantee”).

RECITALS

- A. The City wishes to enter into this Agreement with Grantee to provide funding to Grantee to purchase security cameras to be granted to recipient businesses (“Recipients”) throughout designated commercial corridors in East Oakland. The data from the cameras will not be collected or maintained by the City. The data collected by Recipients will not be considered public record. Footage will only be shared with the Oakland Police Department (“OPD”) in the investigation of a crime or with the Oakland Public Works Department (“OPW”) in the investigation of illegal dumping, pursuant to the guidelines of the existing Security Camera Registry and Illegal Dumping Surveillance programs. Signs will be placed in the camera locations advising people that the area is under video surveillance.
- B. The City Council, pursuant to Resolution No. [TBD] C.M.S. has allocated grant funds to Grantee to fund its community-related programs and activities as specified herein.

Now therefore the parties to this Agreement agree as follows:

1. Grant

Subject to the terms and conditions of this Agreement, the City agrees to provide a grant of funds to Grantee in an amount up to one hundred and fifty thousand dollars (\$150,000.00) (the “Grant”).

2. Scope of Work

As a condition of this Grant, Grantee must diligently and in good faith perform the community-related work, services, and activities (“Work”) specified in the **Scope of Work** attached to this Agreement as **Schedule A** and incorporated herein by reference.

Grantee shall designate an individual who shall be responsible for communications with the City for the duration of this Agreement. The Project Manager for the City shall be **Juno Thomas**.

3. Agreement Documents and Provisions

Grantee shall perform or arrange for the performance of Work under this Agreement in accordance with conditions of this Agreement including the attached Scope of Work in addition to City of Oakland rules, regulations and policies and applicable federal and state laws.

4. Time of Performance

The Grant term shall begin on [DATE/TBD] and shall end upon total grant disbursement and/or use, or upon either party's 30-day written notice.

5. Method of Payment

Grantee shall be paid for the performance of the Work set forth in the Scope of Work in accordance with the Program Budget included in the Scope of Work. Payments shall be made in the amounts stated in the Scope of Work and shall be based on actual eligible costs, fees and expenses incurred by Grantee for the Work. Payments shall be due upon completion of the Work or as otherwise specified in the Scope of Work. Grantee shall submit an invoice accompanied by an itemization of expenditures submitted for reimbursement prepared on the City's expense forms. Invoices shall state a description of the Work completed, itemized costs, fees and expense and the amount due.

The documents submitted shall be reviewed and approved for payment by the Project Manager. The City shall have sole and absolute discretion to determine the sufficiency of supporting documentation for payment. Determination of satisfactory completion of the Scope of Work will be based on an overall assessment of the progress Grantee has made towards achieving the goals of the Agreement and the performance measures.

All authorized obligations incurred in the performance of the terms of this Agreement must be reported to the City within 30 days following the completion or termination of this Agreement. No claims submitted after the 30-day period will be recognized as binding upon the City for payment. Any obligations and/or debts incurred by Grantee and not reported to the City within the 30-day period become the sole liability of Grantee, and the City shall be relieved of any and all responsibilities.

6. Prompt Payment

This Agreement is subject to the Prompt Payment Ordinance codified in Chapter 2.06 of the Oakland Municipal Code. Under said Ordinance, the City must disburse Grant funds to Grantee within 20 business days after receipt of an undisputed request for payment. An undisputed request for payment is a request for payment that is not a "disputed invoice" within the meaning of the Prompt Payment Ordinance. Under the Ordinance, a "disputed invoice" is an invoice or request for payment that is either (1) improperly executed by Grantee, (2) contains errors, (3) requires additional evidence to determine its validity, and/or (4) contains expenditures or proposed expenditures that are ineligible or that do not otherwise comply with reimbursement or disbursement requirements of the City or another grant funding source. If a request for payment is "disputed", the payment/disbursement shall not be subject to late penalties until the dispute is resolved. In the event a request for payment is disputed, the City shall notify Grantee and the City's Liaison (as defined in the Prompt Payment Ordinance) in writing within five business days of receiving the disputed request for payment that there is a bona fide dispute, in which case the City shall withhold the disputed amount

and may withhold the full amount if the funding source for the Grant requires that the disputed expenditures be fully resolved prior to any disbursement of Grant funds. If the funding source for the Grant requires its review and approval before payments are made to Grantee, this period shall be suspended for any period of review by said agency. If any amount due by the City to be disbursed to Grantee pursuant to this Agreement is not timely paid in accordance with the Prompt Payment Ordinance, Grantee is entitled to interest penalty in the amount of 10% of the improperly withheld amount per year for every month that payment is not made, provided that Grantee agrees to release the City from any and all further claims for interest penalties that may be claimed or collected on the amount due and paid. Grant recipients that receive interest penalties for late payment pursuant to the Prompt Payment Ordinance may not seek further interest penalties on the same late payment in law or equity.

The Prompt Payment Ordinance further requires that, unless specific exemptions apply, Grantee shall pay undisputed invoices of its subcontractors for goods and/or services within 20 business days of submission of invoices unless Grantee notifies the City's Liaison in writing within five business days that there is a bona fide dispute between Grantee and claimant, in which case Grantee may withhold the disputed amount but shall pay the undisputed amount. Disputed payments are subject to investigation by the City's Liaison and, upon the filing of a compliant, Grantee, if opposing payment, shall provide security in the form of cash, certified check or bond to cover the disputed amount and penalty during the investigation. If Grantee fails or refuses to deposit security, the City will withhold an amount sufficient to cover the claim from the next Grant payment. The City, upon a determination that an undisputed invoice or payment is late, will release security deposits or withholds directly to claimants for valid claims. Grantee is not allowed to retain monies from subcontractor payments for goods as project retention, and is required to release subcontractor project retention in proportion to the subcontractor services rendered, for which payment is due and undisputed, within five business days of payment. For the purpose of posting on the City's website, Grantee is required to file notice with the City of release of retention and payment of mobilization fees, within five business days of such payment or release; and Grantee is required to file an affidavit, under penalty of perjury, that he or she has paid all subcontractors, within five business days following receipt of payment from the City. The affidavit shall provide the names and address of all subcontractors and the amount paid to each.

7. Evaluation, Monitoring and Reporting

Grantee shall be monitored and evaluated by the City in terms of its effectiveness and timely compliance with the provisions of this Agreement and the effective and efficient achievement of the Scope of Work. Grantee shall undertake continuous quantitative and qualitative evaluation of the Scope of Work as specified in this Agreement and shall make written reports on the results of such evaluation to the Project Manager as reasonably requested by the Project Manager.

In addition to the financial requirements described elsewhere in this Agreement, Grantee agrees that authorized representatives of the City may perform fiscal monitoring of Grantee's record-keeping and reporting to assure compliance with this Agreement.

Grantee also agrees to be bound and abide by the City's Surveillance Ordinance, Oakland Municipal Code Chapter 9.64, including submission of a Use Policy and Impact Statement for the Camera System that is approved by the Privacy Advisory Commission and the Oakland City Council. Additionally, the Ordinance requires submission of an Annual Surveillance Report. As defined in Chapter 9.64, an Annual Surveillance Report means a written report concerning the grant funded Camera program, that includes all of the following:

- a. A description of how the Camera program was used, including the number of cameras purchased, Recipient businesses contracted with, and locations of security cameras on business premises;
- b. Whether and how often data acquired by the use of the Camera program was directly shared with the City, the name of the Recipient business sharing the data, the types of data disclosed, under what legal standards the information was disclosed and the justification for the disclosures;
- c. Where applicable, a breakdown of what physical objects the Camera program hardware was installed upon, using general terms so as not to disclose the specific location of such hardware; and for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
- d. Where applicable, a breakdown of where the surveillance technology was deployed geographically in the relevant year;
- e. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. This analysis shall also include the race of each person subjected to the technology unless this requirement is waived by the City's Privacy Advisory Commission. If waiver is granted, the annual report will include the written findings in support of this determination;
- f. The results of any internal audits, any information about violations or potential violations of the Camera program Use Policy, and any actions taken in response unless the release of such information is prohibited by law; and
- g. Information about any data breaches or other unauthorized access to the data collected by the Camera program, including information about the scope of the breach and the actions taken in response.
- h. Information, including crime and/or illegal dumping statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;
- i. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;
- j. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
- k. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request. Grantee agrees that should the City find that a violation of Chapter 9.64

has occurred, Grantee will either return the camera equipment or reimburse the City for the cost.

8. Program Income

Any funds received as return of costs or as income generated from activities funded by this Agreement are the property of the City and must be transmitted to the City promptly.

9. Proprietary or Confidential Information of the City

Grantee understands and agrees that, in the performance of the work or services under this Agreement or in contemplation thereof, Grantee may have access to private or confidential information which may be owned or controlled by the City and that such information may contain proprietary or confidential details, the disclosure of which to third parties may be damaging to the City. Grantee agrees that all information disclosed by the City to Grantee shall be held in confidence and used only in performance of the Agreement. Grantee shall exercise the same standard of care to protect such information as a reasonably prudent Grantee would use to protect its own proprietary data.

10. Records and Audit

Grantee must maintain (a) a full set of accounting records in accordance with generally accepted accounting principles and procedures for all funds received under this Agreement, and (b) full and complete documentation of performance related matters such as benchmarks and deliverables associated with this Agreement. Grantee agrees to comply with all audit, inspection, record-keeping and fiscal reporting requirements mandated by the City, and all state and/or federal audit requirements applicable to the funding sources of the Grant. The City shall notify the Grantee of any records it deems in its reasonable judgment to be insufficient. Grantee shall have 15 calendar days from such notice to correct any specified deficiency in the records, or, if more than 15 days shall be reasonably necessary to correct the deficiency, Grantee shall begin to correct the deficiency within 15 days and correct the deficiency as soon as reasonably possible. Grantee must maintain such records for a period of four years following the last fiscal year during which the City paid an invoice to Grantee under this Agreement.

Grantee must make available at Grantee's office for examination at reasonable intervals and during normal business hours to the City's representatives, as well as representatives of agencies providing funding for the Grant, all books, accounts, reports, files, financial records, and other papers or property with respect to all matters covered by this Agreement, as well as the financial condition of Grantee in general, and shall permit these representatives to audit, examine, and make copies, excerpts or transcripts from such records. The City's representatives may make audits of any conditions relating to this Agreement, as well as the financial condition of Grantee in general, throughout the term of this Agreement and for three years following the expiration of the term of this Agreement.

11. Fraud, Waste and Abuse

Grantee must immediately inform the City of any information or complaints involving criminal fraud, waste, abuse, or other criminal activity in connection with the Work.

12. Compliance with Federal Standards

Not Applicable.

13. Assignment and Subcontracting

Grantee may not assign, subcontract, or otherwise transfer any rights, duties, obligations or interest in this Grant or Agreement or arising hereunder to any person, persons, entity or entities whatsoever without the prior written consent of the City, and any attempt to assign, subcontract, or transfer without such prior written consent shall be void. Consent to any single assignment, subcontract, or transfer shall not constitute consent to any further assignment, subcontract or transfer.

14. Publicity

Any publicity generated by Grantee for the program funded pursuant to this Agreement, during the term of this Agreement or for one year thereafter, shall make reference to the contribution of the City in making the project possible. The words "City of Oakland" shall be explicitly stated in all pieces of publicity, including but not limited to flyers, press releases, posters, brochures, public service announcements, interviews and newspaper articles.

City staff will be available whenever possible at the request of Grantee to assist Grantee in generating publicity for the program funded pursuant to this Agreement. Grantee further agrees to cooperate with authorized City officials and staff in any City-generated publicity or promotional activities undertaken with respect to this program.

15. Insurance

Unless a written waiver is obtained from the City's Risk Manager, Grantee must provide the insurance listed in the City of Oakland **Insurance Requirements** attached hereto as **Schedule Q** and incorporated herein by reference.

16. Indemnification

- a. Notwithstanding any other provision of this Agreement, Grantee shall indemnify and hold harmless (and at City's request, defend) the City, and its Councilmembers, officers, partners, agents, and employees (each of which persons and organizations are referred to collectively herein as "Indemnitees" or individually as "Indemnitee") from and against any and all liabilities, claims, lawsuits, losses, damages, demands, debts, liens, costs, judgments, obligations, administrative or regulatory fines or penalties, actions or causes

of action, and expenses (including reasonable attorneys' fees) caused by or arising out of any:

- (i) Breach of Grantee's obligations, representations or warranties under this Agreement;
 - (ii) Act or failure to act in the course of performance by Grantee under this Agreement;
 - (iii) Negligent or willful acts or omissions in the course of performance by Grantee under this Agreement;
 - (iv) Claim for personal injury (including death) or property damage to the extent based on the strict liability or caused by any negligent act, error or omission of Grantee;
 - (v) Unauthorized use or disclosure by Grantee of confidential information; or
 - (vi) Claim of infringement or alleged violation of any United States patent right or copyright, trade secret, trade mark, or service mark or other proprietary or intellectual property rights of any third party.
- b. For purposes of the preceding subsections (i) through (vi), the term "Grantee" includes Grantee, its officers, directors, employees, representatives, agents, servants, sub-consultants and subgrantees.
- c. The City shall give Grantee prompt written notice of any such claim of loss or damage and shall cooperate with Grantee, in the defense and all related settlement negotiations to the extent that cooperation does not conflict with City's interests.
- d. Notwithstanding the foregoing, the City shall have the right if Grantee fails or refuses to defend the City with counsel acceptable to the City to engage its own counsel for the purposes of participating in the defense. In addition, the City shall have the right to withhold any payments due Grantee in the amount of anticipated defense costs plus additional reasonable amounts as security for Grantee's obligations under this section. In no event shall Grantee agree to the settlement of any claim described herein without the prior written consent of the City.
- e. Grantee acknowledges and agrees that it has an immediate and independent obligation to indemnify and defend Indemnitees from any claim or action which potentially falls within this indemnification provision, which obligation shall arise at the time such claim is tendered to Grantee by the City and continues at all times thereafter, without regard to any alleged or actual contributory negligence of any Indemnitee. Notwithstanding anything to the contrary contained herein, Grantee's liability under this Agreement shall not apply to any action or claim arising from the sole negligence, active negligence, or willful misconduct of an Indemnitee.
- f. All of Grantee's obligations under this section are intended to apply to the fullest extent permitted by law (including without limitation, California Civil Code Section 2782) and shall survive the expiration or sooner termination of this Agreement.

- g. The indemnity set forth in this section shall not be limited by the City's insurance requirements contained in Schedule Q hereof, or by any other provision of this Agreement. The City's liability under this Agreement shall be limited to payment of Grantee in accord to the terms and conditions under this Agreement and shall exclude any liability whatsoever for consequential or indirect damages even if such damages are foreseeable.

17. Non-Liability of City

No member, official, officer, director, employee, or agent of the City shall be liable to Grantee for any obligation created under the terms of this Agreement except in the case of actual fraud or willful misconduct by such person.

18. Right to Offset Claims for Money

All claims for money due or to become due from the City shall be subject to deduction or offset by the City from any monies due Grantee by reason of any claim or counterclaim arising out of this Agreement, any purchase order, or any other transaction with Grantee.

19. Events of Default and Remedies

The occurrence of any of the following shall constitute a material default and breach of this Agreement by Grantee:

- a. Failure to adequately perform the Work set forth in the Scope of Work;
- b. Improper use or reporting of funds provided under this Agreement by Grantee or its employees or agents;
- c. Substantial failure by Grantee to observe and perform any other provision of this Agreement; or
- d. Grantee's (1) filing for bankruptcy, dissolution, or reorganization, or failure to obtain a full dismissal of any such involuntary filing brought by another party before the earlier of final relief or 60 days after the filing; (2) making a general assignment for the benefit of creditors; (3) applying for the appointment of a receiver, trustee, custodian, or liquidator, or failure to obtain a full dismissal of any such involuntary application brought by another party before the earlier of final relief or 60 days after the filing; (4) insolvency; or (5) failure, inability or admission in writing of its inability to pay its debts as they become due.

The City shall give written notice to Grantee or Grantee's agent of any default by specifying (a) the nature of the event or deficiency giving rise to the default, (b) the action required to cure the deficiency, if an action to cure is possible, and (c) a date, which shall be not less than 30 calendar days from the mailing of the notice, by which such action to cure, if a cure is possible, must be undertaken. Grantee shall not be in default if Grantee cures such default within the specified cure period, or, if such default is not reasonably capable of cure within the specified period, Grantee begins to cure the default within the cure period and thereafter diligently pursues the cure to completion. Following any notice of an event of default, the

City may suspend payments under this Agreement pending Grantee's cure of the specified breach. Upon an event of default that has not been cured by Grantee, the City, in its discretion, may take any of the following actions:

- (A) Terminate this Agreement in whole or in part;
- (B) Suspend payments under this Agreement;
- (C) Demand immediate reimbursement of any funds disbursed under this Agreement;
- (D) Bring an action for equitable relief (a) seeking the specific performance by Grantee of the terms and conditions of the Agreement, and/or (b) enjoining, abating, or preventing any violation of said terms and conditions, and/or (c) seeking declaratory relief;
- (E) Bar Grantee from future funding by the City; and/or
- (F) Pursue any other remedy allowed at law or in equity.

Unless otherwise terminated as provided in this Agreement, this Agreement will terminate on upon total grant disbursement and/or use, or upon either party's 30-day written notice.

20. Termination or Modification for Lack of Appropriation

The City's obligations under this Agreement are contingent upon the availability of funds from the funding source for this Grant. The City may terminate this Agreement on 30 days' written notice to Grantee without further obligation if said funding is withdrawn or otherwise becomes unavailable for continued funding of the Work.

21. Litigation and Pending Disputes

Grantee shall promptly give notice in writing to the City of any litigation pending or threatened against Grantee in which the amount claimed is in excess of \$50,000. Grantee shall disclose, and represents that it has disclosed, any and all pending disputes with the City prior to execution of this Agreement on **Schedule K**, incorporated herein by reference. Failure to disclose pending disputes prior to execution of this Agreement shall be a basis for termination of this Agreement.

22. Conflict of Interest

- a. Grantee certifies that no member, officer, or employee of the City or its designees or agents, and no other public official of the City who exercises any functions or responsibilities with respect to the programs or projects covered by this Agreement, shall have any interest, direct or indirect in this Agreement, or in its proceeds during his/her tenure or for one year thereafter.
- b. Grantee warrants and represents, to the best of its present knowledge, that no public official or employee of City who has been involved in the making of this Agreement, or who is a member of a City board or commission which has been involved in the making of this Agreement whether in an advisory or decision-

making capacity, has or will receive a direct or indirect financial interest in this Agreement in violation of the rules contained in California Government Code Section 1090 et seq., pertaining to conflicts of interest in public contracting. Grantee shall exercise due diligence to ensure that no such official will receive such an interest.

- c. Grantee further warrants and represents, to the best of its present knowledge and excepting any written disclosures as to these matter already made by Grantee to City, that (1) no public official of City who has participated in decision-making concerning this Agreement or has used his or her official position to influence decisions regarding this Agreement, has an economic interest in Grantee or this Agreement, and (2) this Agreement will not have a direct or indirect financial effect on said official, the official's spouse or dependent children, or any of the official's economic interests. For purposes of this paragraph, an official is deemed to have an "economic interest" in (a) any for-profit business entity in which the official has a direct or indirect investment worth \$2,000 or more, (b) any real property in which the official has a direct or indirect interest worth \$2,000 or more, (c) any for-profit business entity in which the official is a director, officer, partner, trustee, employee or manager, or (d) any source of income or donors of gifts to the official (including nonprofit entities) if the income totaled more than \$500, or value of the gift totaled more than \$500 the previous year. Grantee agrees to promptly disclose to the City in writing any information it may receive concerning any such potential conflict of interest. Grantee's attention is directed to the conflict of interest rules applicable to governmental decision-making contained in the Political Reform Act (California Government Code Section 87100 et seq.) and its implementing regulations (California Code of Regulations, Title 2, Section 18700 et seq.).
- d. Grantee shall incorporate or cause to be incorporated into all subcontracts for work to be performed under this Agreement a provision governing conflict of interest in substantially the same form set forth herein.
- e. Nothing herein is intended to waive any applicable federal, state or local conflict of interest law or regulation.
- f. In addition to the rights and remedies otherwise available to the City under this Agreement and under federal, state and local law, Grantee understands and agrees that, if the City reasonably determines that Grantee has failed to make a good faith effort to avoid an improper conflict of interest situation or is responsible for the conflict situation, the City may (1) suspend payments under this Agreement, (2) terminate this Agreement, and/or (3) require reimbursement by Grantee to the City of any amounts disbursed under this Agreement. In addition, the City may suspend payments or terminate this Agreement whether or not Grantee is responsible for the conflict of interest situation.

23. Non-Discrimination/Equal Employment Practices

Grantee shall not discriminate or permit discrimination against any person or group of persons in any manner prohibited by federal, state or local laws. During the performance of this Agreement, Grantee agrees as follows:

- a. Grantee and Grantee's subgrantees, if any, shall not discriminate against any employee or applicant for employment because of actual or perceived age, marital or familial status, religion, gender, gender identity, gender expression, sexual orientation, race, creed, color, genetic information, ancestry national origin, physical or mental disability including Acquired-Immune Deficiency Syndrome (AIDS) or AIDS-Related Complex (ARC), or military status. This nondiscrimination policy shall include, but not be limited to, the following: employment, upgrading, failure to promote, demotion or transfer, recruitment advertising, layoffs, termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.
- b. Grantee and Grantee's subgrantees shall state in all solicitations or advertisements for employees placed by or on behalf of Grantee that all qualified applicants will receive consideration for employment without regard to actual or perceived age, marital or familial status, religion, gender, gender identity, gender expression, sexual orientation, race, creed, color, genetic information, ancestry, national origin, physical or mental disability including Acquired-Immune Deficiency Syndrome (AIDS) or AIDS-Related Complex (ARC), or military status.
- c. Grantee shall make its goods, services, and facilities accessible to people with disabilities and shall verify compliance with the Americans with Disabilities Act by executing **Schedule C-1, Declaration of Compliance with the Americans with Disabilities Act**, attached hereto and incorporated herein.
- d. If applicable, Grantee will send to each labor union or representative of workers with whom Grantee has a collective bargaining agreement or contract or understanding, a notice advising the labor union or workers' representative of Grantee's commitments under this nondiscrimination clause and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

24. Local/Small Local Enterprise Participation

The City has established requirements for participation by local and small local enterprises, including local nonprofit organizations and small local nonprofit organizations, in publicly-supported projects. Unless otherwise indicated, the City acknowledges that Grantee complies with this requirement.

25. Living Wage Requirements

Grantee will be considered a City Financial Assistance Recipient (“CFAR”) and must comply with the Oakland Living Wage Ordinance if it receives \$100,000 or more in financial assistance from the City during a 12-month period. The Living Wage Ordinance requires that nothing less than a prescribed minimum level of compensation (a living wage) be paid to employees of CFARs (OMC 2.28, Ord. 1250 § 1, 1998). The Ordinance also requires submission of the Declaration of Compliance attached and incorporated herein as **Schedule N** and made part of this Agreement, and, unless specific exemptions apply or a waiver is granted, that Grantee provide the following to its employees who perform services under or related to this Agreement:

- a. Minimum compensation – Said employees shall be paid an initial hourly wage rate of **\$14.98 with health benefits and \$17.19 without health benefits**. These initial rates shall be upwardly adjusted each year no later than April 1 in proportion to the increase at the immediately preceding December 31 over the year earlier level of the Bay Region Consumer Price Index as published by the Bureau of Labor Statistics, U.S. Department of Labor. Effective July 1st of each year, Grantee shall pay adjusted wage rates.
- b. Health benefits – Said full-time and part-time employees paid at the lower living wage rate shall be provided health benefits of at least \$2.21 per hour. Grantee shall provide proof that health benefits are in effect for those employees no later than 30 days after execution of the contract or receipt of City financial assistance.
- c. Compensated days off – Said employees shall be entitled to twelve compensated days off per year for sick leave, vacation or personal necessity at the employee's request, and ten uncompensated days off per year for sick leave. Employees shall accrue one compensated day off per month of full time employment. Part-time employees shall accrue compensated days off in increments proportional to that accrued by full-time employees. The employees shall be eligible to use accrued days off after the first six months of employment or consistent with company policy, whichever is sooner. Paid holidays, consistent with established employer policy, may be counted toward provision of the required 12 compensated days off. Ten uncompensated days off shall be made available, as needed, for personal or immediate family illness after the employee has exhausted his or her accrued compensated days off for that year.
- d. Federal Earned Income Credit (EIC) – Grantee shall inform employees that he or she may be eligible for EIC and shall provide forms to apply for advance EIC payments to eligible employees.
- e. Grantee shall provide to all employees and to the Office of Contract Compliance, written notice of its obligation to eligible employees under the City’s Living Wage requirements. Said notice shall be posted prominently in communal areas of the work site(s) and shall include the above-referenced information.

- f. Grantee shall provide all written notices and forms required above in English, Spanish or other languages spoken by a significant number of employees within 30 days of employment under this Agreement.
- g. Reporting – Grantee shall maintain a listing of the name, address, hire date, occupation classification, rate of pay and benefits for each of its employees. Grantee shall provide a copy of said list to the Office of Contract Compliance, on a quarterly basis, by March 31, June 30, September 30 and December 31 for the applicable compliance period. Failure to provide said list within five days of the due date will result in liquidated damages of five hundred dollars (\$500.00) for each day that the list remains outstanding. Grantee shall maintain employee payroll and related records for a period of four (4) years after expiration of the compliance period.
- h. Grantee shall require subgrantees that provide services under or related to this Agreement to comply with the above Living Wage provisions. Grantee shall include the above-referenced sections in its subcontracts. Copies of said subcontracts shall be submitted to the Office of Contract Compliance.

26. Equal Benefits Ordinance

This Agreement is subject to the Equal Benefits Ordinance codified in Chapter 2.32 of the Oakland Municipal Code and its implementing regulations. The purpose of this Ordinance is to protect and further the public, health, safety, convenience, comfort, property and general welfare by requiring that public funds be expended in a manner so as to prohibit discrimination in the provision of employee benefits by City grantees between employees with spouses and employees with domestic partners, and/or between domestic partners and spouses of such employees.

The Ordinance shall only apply to those portions of a Grantee's operations that occur (1) within the City of Oakland; (2) on real property outside the City of Oakland if the property is owned by the City or if the City has a right to occupy the property, and if the contract's presence at that location is connected to a contract with the City; and (3) elsewhere in the United States where work related to a City contract is being performed. The requirements of this chapter shall not apply to subcontracts or subgrantees of Grantee.

The Equal Benefits Ordinance requires, among other things, submission of the Equal Benefits Declaration of Nondiscrimination attached hereto as **Schedule N-1** and incorporated herein by reference.

27. Minimum Wage Ordinance

Oakland employers are subject to Oakland's Minimum Wage Law, whereby Oakland employees must be paid the current Minimum Wage rate.

Employers must notify employees of the annually adjusted rates by each December 15th and prominently display notices at the job site.

The law requires paid sick leave for employees and payment of service charges collected for their services.

28. Political Prohibition

Subject to applicable State and Federal laws, moneys paid pursuant to this Agreement shall not be used for political purposes, sponsoring or conducting candidate's meetings, engaging in voter registration activity, nor for publicity or propaganda purposes designed to support or defeat legislation pending before federal, state or local government.

29. Religious Prohibition

There shall be no religious worship, instruction, or proselytization as part of, or in connection with the performance of the Agreement.

30. Business Tax Certificate or Exemption

Grantee shall obtain and provide proof of a valid City business tax certificate or business tax exemption certificate. Said certificate must remain valid during the duration of this Agreement.

31. Abandonment of Grant

The City may abandon or indefinitely postpone the Grant at any time. Should the Grant be abandoned, the City shall pay Grantee for all services performed thereto in accordance with the terms of this Agreement.

32. Relationship of Parties

The relationship of the City and Grantee is solely that of a grantor and grantee of funds, and should not be construed as a joint venture, equity venture, partnership, or any other relationship. The City does not undertake or assume any responsibility or duty to Grantee (except as provided for herein) or to any third party with respect to the Work performed under this Agreement. Except as the City may specify in writing, Grantee has no authority to act as an agent of the City or to bind the City to any obligation.

33. Warranties

Grantee represents and warrants: (1) that it has access to professional advice and support to the extent necessary to enable Grantee to fully comply with the terms of this Agreement and otherwise carry out the Work; (2) that it is duly organized, validly existing and in good standing under the laws of the State of California; (3) that it has the full power and authority to undertake the Work; (4) that there are no pending or threatened actions or proceedings before any court or administrative agency which may substantially affect the financial condition or operation of the Grantee, other than those already disclosed to the City; and (5) that the persons executing and delivering this Agreement are authorized to execute and deliver such document on behalf of Grantee.

34. Unavoidable Delay in Performance

The time for performance of provisions of this Agreement by either party shall be extended for a period equal to the period of any delay directly affecting this Agreement which is caused by: war; insurrection; strikes; lock-outs; riots; floods; earthquakes; fires; casualties; acts of God; acts of a public enemy; epidemics; quarantine restrictions; freight embargoes; lack of transportation; suits filed by third parties concerning or arising out of this Agreement; or unseasonable weather conditions. An extension of time for any of the above-specified causes will be deemed granted only if written notice by the party claiming such extension is sent to the other party within ten calendar days from the commencement of the cause. Times of performance under this Agreement may also be extended for any cause for any period of time by the mutual written agreement of the City and Grantee.

35. Validity of Contracts

This Agreement shall not be binding or of any force or effect until it is approved for form and legality by the Office of the City Attorney and signed by the City Administrator or his or her designee.

36. Governing Law

This Agreement shall be interpreted under and be governed by the laws of the State of California, except for those provisions relating to choice of law or those provisions preempted by federal law or expressly governed by federal law.

37. Notice

If either party shall desire or be required to give notice to the other, such notice shall be given in writing, via facsimile and concurrently by prepaid U.S. certified or registered postage, addressed to recipient as follows:

City
City of Oakland
Economic and Workforce Development Department
250 Frank Ogawa Plaza, Suite 5313
Oakland, CA 94612
Attn:

Grantee
TBD

Any party to this Agreement may change the name or address of representatives for purpose of this Notice paragraph by providing written notice to all other parties ten (10) business days before the change is effective.

38. Entire Agreement of the Parties

This Agreement supersedes any and all agreements, either oral or written, between the parties with respect to this Grant and contains all of the representations, covenants and agreements between the parties with respect to the Grant. Each party to this Agreement acknowledges that no representations, inducements, promises or agreements, orally or otherwise, have been made by any party, or anyone acting on behalf of any party which are not contained in this Agreement, and that no other agreement, statement or promise not contained in this Agreement will be valid or binding.

39. Amendments and Modifications

Any amendment to or modification of this Agreement will be effective only if it is in a writing signed by all parties to this Agreement.

40. Waiver

Any waiver by the City of an obligation in this Agreement must be in writing and must be executed by an authorized agent of the City. No waiver should be implied from any delay or failure by the City to take action on any breach or event of default of Grantee or to pursue any remedy allowed under this Agreement or applicable law. Any extension of time granted to Grantee to perform any obligation under this Agreement will not operate as a waiver or release from any of its obligations under this Agreement. Consent by the City to any act or omission by Grantee should not be construed to be a consent to any other act or omission or to waive the requirement for the City's written consent to future waivers.

41. Other Agreements

Grantee represents that it has not entered into any agreements that are inconsistent with the terms of this Agreement. Grantee may not enter into any agreements that are inconsistent with the terms of this Agreement without an express written waiver by the City.

42. Severability/Partial Invalidity

If any term or provision of this Agreement, or the application of any term or provision of this Agreement to a particular situation, shall be finally found to be void, invalid, illegal or unenforceable by a court of competent jurisdiction, then notwithstanding such determination, such term or provision shall remain in force and effect to the extent allowed by such ruling and all other terms and provisions of this Agreement or the application of this Agreement to other situation shall remain in full force and effect.

Notwithstanding the foregoing, if any material term or provision of this Agreement or the application of such material term or condition to a particular situation is finally found to be void, invalid, illegal or unenforceable by a court of competent jurisdiction, then the parties hereto agree to work in good faith and fully cooperate with each other to amend this Agreement to carry out its intent.

43. Commencement, Completion and Close-out

It shall be the responsibility of Grantee to coordinate and schedule the Work to be performed so that commencement and completion take place in accordance with the provisions of this Agreement. Any time extension granted to Grantee to enable Grantee to complete the Work must be in writing and shall not constitute a waiver of rights the City may have under this Agreement. Should Grantee not complete the Work by the scheduled date or by an extended date, the City shall be released from all of its obligations under this Agreement.

Within thirty (30) days of completion of the performance under this Agreement, Grantee shall make a determination of any and all final costs due under this Agreement and shall submit a requisition for such final and complete payment (including without limitations any and all claims relating to or arising from this Agreement) to the City. Failure of Grantee to timely submit a complete and accurate requisition for final payment shall relieve the City of any further obligations under this Agreement, including without limitation any obligation for payment of work performed or payment of claims by Grantee.

44. Consents and Approvals

Any consent or approval required under this Agreement may not be unreasonably withheld, delayed, or conditioned.

45. Inconsistency

If there is any inconsistency between the main agreement and the attachments/exhibits, the text of the main agreement shall prevail.

46. Counterparts

This Agreement may be signed in multiple counterparts, which, when signed by all parties, will constitute a binding agreement.

47. Exhibits

The following exhibits and schedules are attached to this Agreement and are hereby incorporated herein by reference:

- Schedule A: Scope of Work and Budget
- Schedule C-1: Compliance with ADA
- Schedule K: Pending Dispute Disclosure Form
- Schedule N: Declaration of Compliance with Living Wage
- Schedule N-1: Equal Benefits, Declaration of Nondiscrimination
- Schedule Q: Insurance Requirements

48. Approval

If the terms of this Agreement are acceptable to Grantee and the City, sign and date below.

[SIGNATURES ON NEXT PAGE]

DRAFT

“CITY”

CITY OF OAKLAND, a municipal corporation

By: _____
City Administrator (date)

Approved for forwarding:

By: _____
Department Head (date)

Resolution Number

Approved as to form and legality:

By: _____
Deputy City Attorney

“GRANTEE”

By: _____

Name: _____

Title: _____ AUTHORIZED OFFICER OF ORGANIZATION _____

Date: _____

GRANT AGREEMENT

EXHIBIT A

SCOPE OF WORK AND BUDGET

*[Scope of Work to incorporate Use Policy and Impact Analysis,
as reviewed and approved by the Privacy Advisory Commission]*

DRAFT



DEPARTMENTAL GENERAL ORDER

I 29: CRIME ANALYSIS SOFTWARE

Effective Date:

Coordinator: Criminal Investigations Division, Crime Analysis Unit

CRIME ANALYSIS SOFTWARE

The purpose of this order is to establish Departmental policy and procedures for the use of Crime Analysis Software.

A. VALUE STATEMENT

The purpose of this policy is to establish guidelines for the Oakland Police Department's (OPD) use of crime analysis software. The OPD Crime Analysis Section, part of the Criminal Investigations Division (CID), uses crime analysis software to examine crime patterns and provide OPD personnel with timely and useful information to assist in reducing crime in Oakland.

B. Purpose of the Technology: *The specific purpose(s) that the surveillance technology is intended to advance*

OPD uses information from the Crime Analysis Section to make data-informed decisions on how to deploy its limited resources toward reducing crime and completing investigations. Crime that occurs each year in Oakland can be analyzed by dedicated crime analysts, who manually interpret trends and patterns. This analysis helps OPD commanders undertake proactive approaches to crime deterrence. Data-driven analysis is one of the hallmarks of modern policing. Crime data analysis helps OPD deploy limited personnel effectively, while avoiding random deployments that may negatively impact Oakland communities. Police departments need geographical analytic technology to illuminate crime trends and uncover actionable information for crime investigations.

C. Description of The Technology: *the information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data.*

OAKLAND POLICE DEPARTMENT

Crime analysis software, such as CentralSquare's CrimeView product suite,¹ comprises specialized applications for dedicated crime analysts. Analysts with these unique software applications can use them to integrate OPD's computer-aided dispatch (CAD) and law enforcement records management system (LRMS) data into a geographical interface, such as ESRI's ArcGIS² (geographic information system) enterprise mapping software. These applications use only internal OPD databases, primarily the CAD and LRMS systems. They can be connected to other internal OPD databases, such as OPD's gunshot location detection system (ShotSpotter) application.³

Crime analysis software lets analysts look at crime types and locations from a holistic geographical perspective. Analysts can view all crimes of a certain type across the entire geography of the city. This lets geographical clustering and patterning emerge that wouldn't be immediately obvious without viewing the incidents on a map. Queries in this application can be tailored to the entire city down to the beat level, depending on the crime type being analyzed. This type of software assists analysts in manually identifying trends, patterns, and areas with high numbers of specific crimes. Coupled with temporal analysis, the analysts can produce meaningful reports that assist police commanders in making deployment and investigative decisions.

CentralSquare's CrimeView product suite comprises three applications:

- CrimeView Desktop is a specialized desktop application that runs as an extension to ESRI's ArcGIS mapping application. Data is hosted within the City of Oakland's Information Technology Department (ITD);
- CrimeView Analytics is a cloud-based software-as-a-service (SaaS) that is hosted in CentralSquare's CJIS⁴-compliant cloud. This application is available to OPD personnel;
- Crimemapping.com is a public-facing SaaS application that provides a map-based view of crime incidents in Oakland. This application complements the City's already existing ITD-based CrimeWatch open-data initiative.

While personally identifying information (PII) is included in the data, the purpose of the product suite is to identify geographical and temporal trends and patterns. The data is not used to look at individuals as suspects or victims of crime.

¹ OPD relies on CentralSquare's CrimeView at the time of the production of this policy for its crime analysis software needs. OPD may choose a different crime analysis software vendor in the future as technology and OPD Crime Analysis Section needs evolve over time. Any new software product must first be submitted for approval per O.M.C. 9.64 et seq.

² <https://www.esri.com/en-us/arcgis/about-arcgis/overview>

³ [ShotSpotter recently purchased Forensic Logic, which produces CopLink. OPD uses CopLink but no OPD data from CrimeView connects to CopLink via ShotSpotter; these are entirely separate systems. ShotSpotter data can be connected to CrimeView in a one-way integration; there is no migration from CrimeView to ShotSpotter or CopLink.](#)

⁴ CJIS = Criminal Justice Information Services Division: <https://www.fbi.gov/services/cjis>

OAKLAND POLICE DEPARTMENT

This product suite does not contain a predictive component. It is used to assist experienced and trained crime analysts create informed analytical commentary supplemented by temporal and visual information. This information helps OPD commanders make sense of the tremendous amount of crime data generated in Oakland.

D. Authorized Use: *the specific uses that are authorized, and the rules and processes required prior to such use the information that can be collected by the surveillance technology.*

The authorized uses of CentralSquare's CrimeView product suite are as follows:

CrimeView Desktop – This application is a license-based desktop application that is used only by trained and experienced crime analysts. The application is an extension to ESRI's ArcGIS enterprise mapping program. Each crime analyst has ArcGIS installed on his or her computer. The CrimeView Desktop extension is then installed by CentralSquare technicians. Only authorized users may have this application installed on their desktops; all OPD desktop machines require a unique username and password for access. Analysts use the software to manually identify trends, patterns, and areas with high concentrations of specific crimes.

CrimeView Analytics – This application is an OPD-wide SaaS application. Only OPD sworn law enforcement personnel or authorized professional staff may access CrimeView Analytics. Users must be employees of OPD and have passed all appropriate background checks and clearances. CrimeView Analytics users must access the system using a unique username and password. Access is granted and managed by CID management personnel. OPD personnel use the software to manually identify trends, patterns, and areas with high concentrations of specific crimes.

OPD personnel authorized to use CrimeView Desktop and Analytics receive required security awareness training prior to using the system, which includes training to access data in CLETS⁵, the FBI NCIC System,⁶ and NLETS⁷. Users are selected and authorized by OPD, and OPD warrants that all users understand and have been trained in the protection of Criminal Justice Information (CJI) data in compliance with FBI Security Policy. All CrimeView Desktop and Analytics users have received this required training.

Users shall not use or let others use the equipment or database records for any unauthorized purpose; authorized purposes consist only of queries related to

⁵ <https://www.courts.ca.gov/4901.htm>

⁶ <https://irp.fas.org/agency/doj/fbi/is/ncic.htm>

⁷ <https://www.nlets.org/>

OAKLAND POLICE DEPARTMENT

authorized investigations, internal audits, or for crime analysts to produce crime analysis reports.

E. Data Access: *The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information.*

CrimeView Desktop – Authorized users include only (CID commander) approved crime analysts.

CrimeView Analytics – Authorized users include all sworn personnel and OPD professional staff. Users requesting access must be vetted and approved by OPD CID management staff.

OPD data in the CrimeView product suite is owned by OPD and is drawn from OPD's underlying systems. OPD personnel using CrimeView Desktop or Analytics shall follow all access policies that govern the use of those originating OPD technologies.

OPD's Information Technology (IT) Unit shall be responsible ensuring ongoing compatibility of CrimeView's product suite with OPD computers and mobile digital terminal (MDT) computer systems. OPD's IT Unit will assign personnel to be responsible for ensuring system access and coordinate with CentralSquare. CrimeView Analytics users are managed through a centralized account management process by OPD CID management personnel.

F. Data Protection: *The safeguards that protect information from unauthorized access, including encryption and access control mechanisms*

CentralSquare constantly processes large streams of criminal justice information (CJI) and thus must comply with the provisions of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI), the FBI Security Management Act of 2003, and the CJIS Security Policy. CentralSquare, along with its partner at Microsoft Azure Government and the National Law Enforcement Telecommunications System (NLETS), have developed strong CJIS-compliant data security protocols.

CentralSquare maintains a security program for managing access to its clients' data – particularly HIPAA and CJIS information. This includes a pre-employment background check, security training required by Federal CJIS regulations, and criminal background checks and fingerprints required by federal or state regulations.

OAKLAND POLICE DEPARTMENT

- G. Data Retention** *The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;*

CentralSquare's CrimeView product suite follows the data-retention schedules reflective of OPD's data-retention schedules. Data that is deleted from OPD's CAD, LRMS, or other systems will be automatically deleted from the CentralSquare CrimeView product suite system.

- H. Public Access:** *how collected information can be accessed or used by members of the public, including criminal defendants.*

Crimemapping.com is the current name of the public facing component of the CrimeView product suite. This public portal provides the public with a map-based view of crime incidents in the City of Oakland.

Information available to the public via the crimemapping.com application is limited to information that falls under the release of information outlined in the California Public Records act.

- Offense Type (assault, robbery, burglary, theft, and so on)
- Incident Number
- Agency
- Date and time

Location information is not currently displayed in crimemapping.com. This is to protect victim privacy and safety as well as protect ongoing investigation integrity.

Exempted information includes any personally identifying information, including exact address locations, which could compromise ongoing investigations as well as witness or victim safety. Map pins are neutralized to the nearest block address or intersection, so as to protect the privacy of the public in instances where crimes are listed near where people reside.

- I. Third Party Data Sharing:** *if and how other city departments, bureaus, divisions, or non-city entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.*

No non-OPD personnel shall access CrimeView Desktop and Analytics. crimemapping.com is a public-facing application and may be accessed by any member of the public.

OAKLAND POLICE DEPARTMENT

- J. Training:** *the training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, and the category of staff that will provide the training*

All city, county, state, and federal agencies that use information from the CLETS must participate in the California Dept. of Justice's training programs to ensure all personnel are trained in the operation, policies, and regulations of each file that is accessed or updated. Training must include the requirement that CLETS information shall only be obtained in the course of official business. The person receiving this information must have a "right to know" and "need to know" and be trained in the possible sanctions and criminal and civil liabilities if the information is misused.

Training shall be provided only by the CA Dept. of Justice's training staff or another certified CLETS/NCIC trainer. At OPD, this four-hour in-person (or live virtual) training is administered by the Communications Division.

Specifically, the training includes the following:

- Initially (within six months of employment or assignment), OPD personnel must attend the four-hour in-person (or live virtual) training.
- Personnel must functionally test and affirm their proficiency with the equipment and operation (full accessor or less than full access, depending on assignment) to ensure compliance with the CLETS and NCIC policies and regulations.

This is accomplished by completing the required training and the appropriate CLETS and NCIC Telecommunications Proficiency Examination published by the California Dept. of Justice.

Biennially, OPD personnel must retest and reaffirm their proficiency to ensure compliance with the CLETS and NCIC policies and regulations. This is accomplished by the completion of the appropriate CLETS and NCIC Telecommunications Proficiency Examination published by the CA DOJ.

- K. Auditing and Oversight:** *the mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.*

OAKLAND POLICE DEPARTMENT

CrimeView Desktop is a single-use licensed desktop application. Auditing and oversight are conducted in-person by CID management personnel. The extension is installed on the Desktop version of ESRI's ArcGIS application. The only individuals that are authorized to use this program are crime analysts working at OPD in the Bureau of Investigations. The installation and use of the extension is overseen by the manager of the Crime Analysis Section. No other individual at OPD is authorized its use. The City's ESRI ArcGIS licensing and maintenance is overseen by the City's GIS section of IDT.

CrimeView Analytics access and use is managed by CID management personnel. Unsuccessful log-on attempts are logged. Inactive users are locked out and cannot be reinstated until they've been re-admitted by the system administrator (an OPD CID management staff member).

- L. Maintenance:** The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

CentralSquare shall be responsible for all SaaS system maintenance per the OPD-CentralSquare contract. OPD and City IDT shall be responsible for all City and OPD-side hardware and software.

By Order of

LeRonne L. Armstrong

Chief of Police

Date Signed:

OAKLAND POLICE DEPARTMENT

Surveillance Impact Report: CrimeView Product Suite

A. Description: The CrimeView Product Suite and Function

The CentralSquare¹ geospatial CrimeView product suite has been the core technology resource for the Oakland Police Department (OPD) crime analysts since 2008. OPD law enforcement personnel and crime analysts have been using CrimeView software for several years. The CrimeView product suite comprises three geospatial applications.

1. CrimeView Desktop is a specialized application for dedicated crime analysts. With this unique software application, analysts can connect to the City's Geographic Information Systems (GIS) ESRI (GIS software vendor) enterprise software ArcGIS (see **Attachment A** for the CrimeView Desktop Operating Manual). Integration with the City's ArcGIS software is a feature that only CentralSquare offers. The connection of CrimeView Desktop with the City's GIS system lets analysts create detailed geographical reports. With this information, police commanders and investigators can make informed, data-driven decisions on how best to reduce crime in Oakland.
2. CrimeView Analytics is an upgrade from the current CrimeView Dashboard product.² This browser-based application connects with OPD incident data to let police officers and commanders access useful geographical data visualizations. CrimeView Analytics lets OPD personnel view data by crime or penal code, by police beat or area, and by time of day and day of week. These data views provide useful crime pattern analysis for officers, OPD commanders, and crime analysts. The CrimeView Analytics upgrade will allow for greater flexibility within the application's paradigm, including support for on-demand queries, scheduled report generation, threshold alerting, and density maps.
3. Crimemapping.com is the public facing application, providing the public with a map-based view of crime incidents in the City of Oakland.³ This application complements the City's already existing IDT-based CrimeWatch open-data initiative.

¹ CrimeView was originally created by the Omega Group, which was later purchased by Tritech. TriTech merged with Central Square in Sept. 2018.

² An online manual for the CrimeView Analytics can be found [here](#).

³ An online manual for the CrimeMapping.com can be found [here](#).

B. Proposed Purpose

CentralSquare's CrimeView product suite (see Attachment B CrimeView Analytics Overview) provides three core services for OPD: 1) a specialized license-based desktop application for crime analysts; 2) a web-based application for OPD personnel; and 3) a public facing geospatial application for the public.

The CrimeView product suite provides geospatial and temporal information, which in turn supports crime analysts' efforts to provide relevant intelligence to OPD's law enforcement personnel. This precision data lets commanders and officers target environments where their intervention results in the most positive impact possible. This data-driven approach to command decision making supports OPD's intelligence-led and precision-based policing initiatives. OPD's data-driven and intelligence-led policing initiatives let OPD minimize the impact of policing across Oakland communities – while still providing police services.

1. CrimeView Desktop – This application is an extension to ESRI's ArcGIS application. This extension lets crime analysts map OPD's crime incident data and use ArcGIS's spatial analysis tools to create detailed reports for OPD officers, investigators, and commanders. This application is only used by crime analysts and requires an advanced working knowledge of ESRI's ArcGIS application and its geospatial analysis tools.

The generated reports provide critical information about crime from a geospatial perspective in an easy-to-view format, including temporal information, which assists in resource deployment and other operational decisions. This application is the workhorse of OPD's Crime Analysis Section, letting analysts provide a depth and breadth of work that would otherwise be impossible. CrimeView Desktop streamlines the geospatial process, saving a huge number of staff hours. This lets analysts use their training and experience to interpret the results and provide critical analytical commentary to support the program's findings.

2. CrimeView Analytics – This web-based application lets police officers and commanders access useful geographical data visualizations by crime or penal code, by police beat or area, and by time of day. These data views provide useful crime pattern analysis for officers, when a detailed, hand-built report may not be necessary. By giving OPD personnel the ability to perform simple visualizations on their own, they are empowered to make operational decisions when a dedicated crime analyst may not be available. Additionally, crime analysts can create snapshot views to give executive team members and area captains a high-level view of crime any time of the day.
3. Crimemapping.com – This application is the public-facing portion of the product suite. It provides a simple map-based view of crime. It is intended for general use; therefore, data is anonymized to protect the privacy of crime victims and the integrity of ongoing investigations. Members of the public can also see other jurisdictions that subscribe to the service and create their own alerts for areas they are concerned about. As mentioned previously, this application complements the City's already existing IDT-based

CrimeWatch open-data initiative.

C. Locations where, and situations in which, the CentralSquare CrimeView product suite may be deployed or used.

The CrimeView product suite is separated into three different applications, so that different groups have access only to the application they are authorized to use.

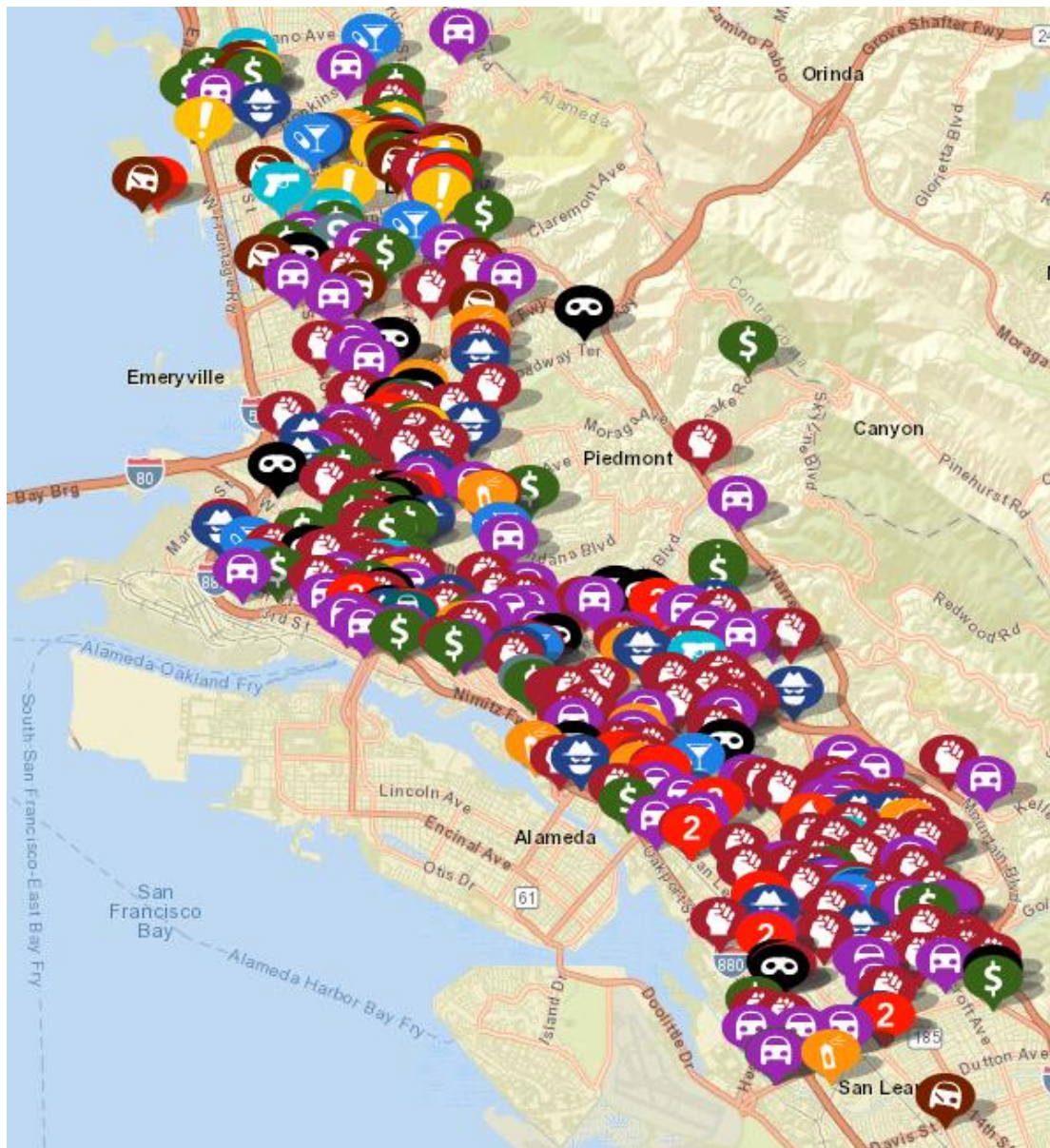
1. CrimeView Desktop – Only crime analysts can use this application, which is an extension to ESRI's ArcGIS desktop mapping application. This license-based software is installed only on devices solely used by crime analysts. These computers are secured within the Police Administration Building (PAB) on floors and in sections that can only be accessed by an employee's keycard. Each employee's network profile is secured, and only authorized employees can access and use CrimeView Desktop.
2. CrimeView Analytics – Only OPD personnel can access this application. OPD personnel are individuals who have undergone a complete background check and have fulfilled the California Department of Justice requirements for using computers on the OPD network. These requirements include, but are not limited to, a written test taken every two years on accessing the California Law Enforcement Telecommunication System (CLETS) and a state-mandated, four-hour in-person training covering the handling and release of confidential information. Everyone using CrimeView Analytics must have his or her own individual login and password; logins cannot be shared. The manager of the Crime Analysis Section personally approves and maintains the list of approved users. Information in CrimeView Analytics is considered internal confidential information, and it cannot be shared with the public – information in Analytics contains information that could compromise, if released, victim privacy and safety as well as compromise ongoing investigations.
3. Crimemapping.com – Any member of the public can access this application. The information displayed in this geospatial application has been formatted to allow the public an anonymized view of crime in Oakland, which protects the privacy and safety of victims and the integrity of ongoing investigations.

Table 1 below provides 2020 and 2021 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland. OPD uses CrimeView Desktop and CrimeView Analytics to better strategize ways to confront the high levels of crime illustrated in this data table. These crimes occur throughout the City, although there are parts of the city that unfortunately see much higher concentrations of violent crime. The CrimeView Desktop and CrimeView Analytics products help OPD commanders and investigators efficiently leverage limited resources to confront areas where crime is most concentrated.

Part 1 Crimes <i>All totals include attempts except homicides</i>	01-01-2020 through 12-31-2020	01-01-2021 through 12-31-2021	Year-to-Date % Change 2020 vs. 2021	3-Year Year-to-Date Average	YTD 2021 vs. 3-Year YTD Average
Homicide - 187(a)	102	124	22%	100	24%
• Homicide - all other *	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• With Firearm	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• Auto	6,221	8,179	31%	8,921	-8%
• Residential	1,247	1,055	-15%	1,370	-23%
• Commercial	958	670	-30%	750	-11%
• Other/Unknown	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

Figure 1 below is a screenshot taken from CrimeMapping.com on March 21, 2022. The CentralSquare product suite includes this public-facing website. Members of the public can use this website to view crime maps and filter by crime type and locations within the City.

Figure 1: Oakland Crimemapping.com Screenshot



D. Impact

The aggregation of data will always cause concern regarding the impact to public privacy. Data used in CentralSquare's CrimeView product suite originates solely from internal OPD database sources – namely the current police records management system (LRMS), including its adjunct field-based reporting module (FBR) and the communications computer-aided dispatch (CAD) system.

The purpose of the CrimeView product suite is to provide geospatial and temporal information about crime incidents, arrests, and calls for service. It uses minimal

personal identifying information, and only in the two applications available to OPD personnel, who are bound by the strict confidentiality rules previously detailed. The personally identifying information is sourced solely from internal OPD database sources and does not include information about an individual's immigration status. Oakland residents who may not have a legal immigration status have a right to privacy. The California Values Act (SB 544) is enacted to ensure that (barring exceptions contained in the law) no state and local resources are used to assist federal immigration enforcement.

CentralSquare complies with all federal (FBI CJIS requirements), state (e.g., SB 54) and local laws (e.g., Oakland Sanctuary City Ordinance⁵) associated with use of collected law enforcement data. This includes, in the state of California and many individual jurisdictions, the prohibition on the use of facial recognition and the analysis of body worn camera video data.

E. Mitigations

OPD and CentralSquare use several strategies to mitigate against the potential for system abuse or data breaches.

System Mitigations

CentralSquare Technologies system provides security for customer data through a layered approach. CentralSquare uses CJIS-level security for storage and access as a best practice for managing customer operational data within. This security includes:

1. Access controls to the application.
2. Secure infrastructure hosted at the hosting facility.
3. Access limited to CentralSquare personnel with the required security approval. Analytics products, such as CrimeView and crimemapping.com, include data imported from their customers' public safety systems (such as CAD and RMS).

The CentralSquare Cybersecurity Program Overview (see Attachment C) "implements a series of comprehensive physical and logical controls that align with the NIST Cyber Security Framework and standards to provide a secure, layered defense for all hosted information. CentralSquare maintains annual Payment Card Industry (PCI) and Statement on Standards for Attestation Engagements (SSAE18) compliance through a series of ongoing assessments and security testing performed by a PCI Qualified Security Assessor and AICPA auditor. Adherence to these standards ensures all controls are met specific to access, transmission, processing, and storage of data."

The CentralSquare Cybersecurity Program overview also explains the framework for secure software development, vulnerability management, security incident

⁴ https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB54

⁵ <https://oakland.legistar.com/LegislationDetail.aspx?ID=3701155&GUID=8153C1B0-B9FC-4B29-BDDE-DF604DEDAEAD&Options=&Search=>

response protocols, government-standard cloud solutions (including audit compliance standards), and regulatory compliance protocols. The CentralSquare Analytics Product Security Overview (**see Attachment D**) provides more security standards.

The City of Oakland-Central Square draft contract (see Attachment E) also provides language on the contractual security system commitments.

Safeguards in Alignment with Oakland and California Immigrant Legal Protections

CentralSquare's CrimeView product suite is geospatial by design. Minimal personally identifying information is only available in CrimeView Desktop and CrimeView Analytics. Use of these two applications is restricted to OPD personnel only, within a specific context. Users can only access these applications if they have a legitimate law-enforcement need for the information.

Data used in CentralSquare's CrimeView product suite originates solely from internal OPD database sources – namely the current police records management system (LRMS), its adjunct field-based reporting module (FBR), and the communications computer-aided dispatch (CAD) system.

Data Access Safeguards

Within the CrimeView Desktop and Analytics applications, OPD data cannot be accessed by anyone outside OPD. Additionally, OPD personnel using the CrimeView Analytics application must have a unique username and password, issued by the Crime Analysis Section manager.

Personnel Oversight

Department General Order (DGO) I 29: CRIME ANALYSIS SOFTWARE, explains that: "While personally identifiable information (PII) is included in the data, the purpose of the product suite is to identify geographical and temporal trends and patterns. The data is not used to look at individuals as suspects or victims of crime."

This product suite does not contain a predictive component. It is used to assist experienced and trained crime analysts create informed analytical commentary supplemented by temporal and visual information. This information helps OPD commanders make sense of the tremendous amount of crime data generated in Oakland. Furthermore, CrimeView Desktop and CrimeView Analytics do not import external data – they only use OPD data that already exists in OPD's internal systems.

Anonymization

Crimemapping.com is accessible by the public. Prior to any data being available via this application, it is anonymized to protect victim privacy and safety as well as the integrity of ongoing investigations.

F. Data Types and Sources

CentralSquare has created a file transfer protocol data feed to automatically acquire data into the CrimeView product suite. This data is currently limited to the police records management system (LRMS), including the adjunct field-based reporting module (FBR), and communications CAD system.

The process by which CrimeView manages and purges expired data is as follows:

- An SQL script is run against the CAD and RMS databases.
- The output is written to a Parquet file and pushed to an S3 bucket in the AWS Government Cloud.
- The Parquet file is read, and the contained data is loaded to the CrimeView SQL database.
- The Parquet files may be kept for several months for troubleshooting purposes but are deleted at regular intervals to enforce data history trimming.
- The CrimeView SQL database is read, and an Elasticube database is rebuilt entirely using the data from SQL. No prior data is retained in the Elasticubes.
- Another synchronization script is run against the CAD and RMS databases to check primary keys and enforce the subscribed date range.

Any records in the CrimeView SQL database that are no longer in the source CAD and RMS database or are earlier than the subscribed date range are subsequently deleted from the CrimeView SQL database.

The following is an exhaustive list of datasets acquired by CentralSquare's CrimeView product suite from OPD data sources:

Data Source Collected	Collection Status	Database Location	Access Conditions
Arrests	Active	LRMS	Only authorized OPD personnel
Field Contacts	Active	LRMS	Only authorized OPD personnel
Incident Reports	Active	LRMS	Only authorized OPD personnel
Calls for Service	Active	CAD	Only authorized OPD personnel
Stop Data	Active	FBR	Only authorized OPD personnel
Traffic Accidents	Active	LRMS	Only authorized OPD personnel

The purpose of the CrimeView product suite is to provide a geospatial view of crime in Oakland. This information assists police personnel, executives, and commanders with resource distribution, operational decisions, and long-term strategies.

G. Data Security

CentralSquare constantly processes large streams of criminal justice information (CJI) and must comply with the provisions of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI), the FBI Security Management Act of 2003, and the CJIS Security Policy.⁶ CentralSquare, along with its partner at Amazon Web Services (AWS) Government have developed strong CJIS-compliant data security protocols.

Supporting documentation from CentralSquare is attached: CentralSquare's Cybersecurity Program Overview and CentralSquare's Analytics Product Security Overview.

- a. Account Management – OPD personnel who use CrimeView Desktop must be seated crime analysts with sole access to their computer and the ArcGIS desktop application with the Desktop extension. OPD personnel who use CrimeView Analytics must have a unique username and password to access the application. The users have access to accounts that are created, deleted, and managed by a local administrator within OPD (the Crime Analysis Section manager), who has special access permissions to the system.
- b. Amazon Web Services (AWS) Government Cloud Protocols – CrimeView cloud data is stored in Amazon Web Services (AWS) Government and encrypted at rest using Microsoft BitLocker. CrimeView Cloud deployments hosted in AWS Government provide encryption through BitLocker (certified FIPS 140-2 encryption components and Microsoft BitLocker FIPS140-2-Jan2017-Certs-2932-2933- 2934).
- c. CrimeView is hosted from an Amazon Web Services (AWS) Government facility. Each facility meets the stringent FBI CJIS Policy standards and guidelines with the following protection features on site:
 - Monitored by both fixed and pan-tilt/zoom security cameras
 - Protected by intrusion detection system
 - Two-factor authentication required for building access
 - Biometric iris authorization required for data center access
 - Extensive pre-employment background investigation process
 - On-site building security and data center monitoring staffed 24/7/365.
- d. User Authentication and Authorization - All authorized users must maintain and enter a valid user ID and strong password combination to gain access to the system. Passwords must be changed every 90 days.
- e. Personnel Screening, Training, and Administration – CrimeView cloud access to implement and support the system is limited to personnel that have completed CentralSquare Technologies' CJIS compliant security approval process:

⁶ <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>

- Access to the Cloud CrimeView infrastructure requires approved personnel to complete a layered secure login process that includes personally assigned passwords, advanced authentication to gain access to the CentralSquare Technologies network, and a secure access login to the applicable Cloud CrimeView domain, application, and SQL Server database.
- Pre-employment background check.
- Security-approved employees must successfully complete the CJIS On-Line Security and Awareness training and testing. Their certifications must be current and must be renewed every two years. In addition to CJIS required training, CentralSquare Technologies also does periodic training for security approved personnel on CentralSquare Technologies security policies.
- Criminal background checks have been completed on CentralSquare Technologies personnel as part of employee screening and by one or more law enforcement agencies (CentralSquare Technologies customers and, in some cases, state law enforcement agencies).
- CentralSquare personnel have been fingerprinted, and their prints have been submitted to one or more law enforcement agencies for a background check.
- Security approved personnel are the same personnel that are used for supporting customers with on-premises deployments of CAD, Mobile, RMS, and other CentralSquare products (including the CrimeView product suite).

H. Costs

A new proposed contract will cost the City \$260,203.00 for the period of January 1, 2022, to December 21, 2026 (approximately \$41,240 per year). The City of Oakland-Central Square draft contract (see **Attachment D**) provides specific contract terms; **Attachment E** provides exact costing details.

I. Third Party Dependence

OPD relies on CrimeView's product suite as a private company to provide OPD with a robust geospatial application environment. The entire product suite, especially CrimeView Desktop, is unique and cannot be mirrored with any internal OPD system.

Section G above explains that Central Square uses Amazon Web Services (AWS) Government for cloud-support services, and that AWS Government has developed strong CJIS-compliant data security protocols. Additionally, Crimemapping.com is hosted in the Microsoft Azure non-government cloud, where only non-sensitive data is stored. Crimemapping.com records are first transmitted to the CrimeView AWS Government cloud then sent to the Crimemapping.com environment in Microsoft Azure. Hosted data at AWS and Azure is encrypted through Microsoft BitLocker and Microsoft FIPS 140-2 compliant encryption is used for data in transit (the same encryption components as CrimeView). Furthermore, CentralSquare also uses SecureLink Remote Access software (www.securelink.com) for remote access. SecureLink meets service

level agreement (SLA) requirements and meets multiple regulatory requirements (such as FIPS and the FBI CJIS Security Policy), while maintaining customer network security.

J. Alternatives Considered

No other product or company can realistically provide OPD with the advanced geospatial functionality required by crime analysts who are creating detailed reports for OPD police personnel.

The CrimeView Desktop extension to ESRI's ArcGIS is unique. No other vendor provides this tool. The CrimeView Desktop application is crucial to the sustained operations of the Crime Analysis Section, letting them focus on analytical observations and expanding the number of work products distributed to key OPD personnel.

K. Track Record of Other Entities

Many other police agencies in the U.S. use the CrimeView product suite (a complete list is not available from the vendor). OPD is aware that the following agencies use the software:

- San Diego Harbor Police. This agency runs an intelligence-led policing strategy using CrimeView Analytics;
- OPD staff has personal experience using the CrimeView product suite while employed by the City of Richmond, CA, as the individual analyst. Having this powerful geospatial application meant that one analyst could serve the entire agency with timely actionable geospatial and temporal information;
- Bedford Police Dept. (Texas);
- St. James Parish Sheriff's Office (Louisiana); and
- Arizona State University Police Dept. (Arizona).

Attachments

- A. Omega Desktop Manual*
- B. CrimeView Analytics Overview*
- C. CentralSquare Cybersecurity Program Overview*
- D. CentralSquare Analytics Product Security Overview*
- E. City of Oakland-Central Square draft contract*
- F. Contract Pricing Document*



Welcome to Omega Desktop 5.2

Omega Desktop is a suite of tools created by The Omega Group to work within ESRI's ArcGIS application. Omega Desktop provides mapping solutions designed to aid decision makers in law enforcement, public safety and education agencies.

The different parts of Omega Desktop include:

CrimeView

CrimeView is an ArcMap extension that provides access to crime data for both novice and advanced users. Novice users, with minimal training, can easily navigate the features of CrimeView by using the simple interface provided. An advanced user can take advantage of the power and flexibility of CrimeView's analysis routines in combination with the analysis capabilities of ArcGIS to produce dynamic maps and reports.

FireView

FireView is an ArcMap extension that provides Fire and Emergency Response Agencies with mapping tools to help review existing deployment policies and develop new strategies. FireView integrates Fire and EMS data with GIS allowing agencies to easily map and analyze data. By identifying incident patterns and response effectiveness, resources can be more optimally redeployed.

School Planner

School Planner is an ArcMap extension that integrates student enrollment data in a mapping environment. School Planner has been developed specifically to meet the needs of a facility planner or demographer to assist in completing detailed enrollment analysis, boundary redistricting and facility planning.

Omega Data Manager

The preparation of accurate source information on which to base geographic analyses is important to the GIS process. The Omega Data Manager contains tools available as an extension to ArcCatalog to assist in preparing standardized, accurate data for use with Omega Desktop routines.

Omega Import Wizard

Fundamental to Geographic Information Systems (GIS) is the data. To produce practical results for mapping and reporting with OmegaGIS, especially where the data is changing frequently from day to day, it is important the data be both accurate and up to date. The Omega Import Wizard provides a standardized, scheduled method for retrieving datasets from Database Management Systems (DBMS) or ASCII files, so that they may be geocoded for use with Omega Desktop and Omega Web applications.

Dashboard

Dashboard is an extension to CrimeView, FireView and School Planner that provides the ability to publish analytical information to the web in the form of maps, graphs or reports. Data is created using Omega Desktop software, and then posted to a web server which serves up the information through a web site. In addition to the web site that is set up to view the content, an administrative web site is provided to organize and manage the content that is published.

Licensing

All Omega Desktop products, CrimeView, FireView, School Planner, Dashboard and the Import Wizard, are protected from unauthorized use. Omega Desktop products are licensed to an individual computer and require a machine specific license. Concurrent licensing is not available.

When Omega software is purchased an installation number will be created for each license of the software. The installation number is prefixed by the letters associated with the product. For instance, an install number for CrimeView will begin with CV2, FireView FV2, School Planner SP2, Dashboard DF2 and Import Wizard IW2. Each installation number should be associated with a specific machine.

Training licenses are available from Omega. A training license will time-out based on the amount of time required for training. Contact an Omega staff member to enquire about training licenses.

[Steps to License a Product](#)

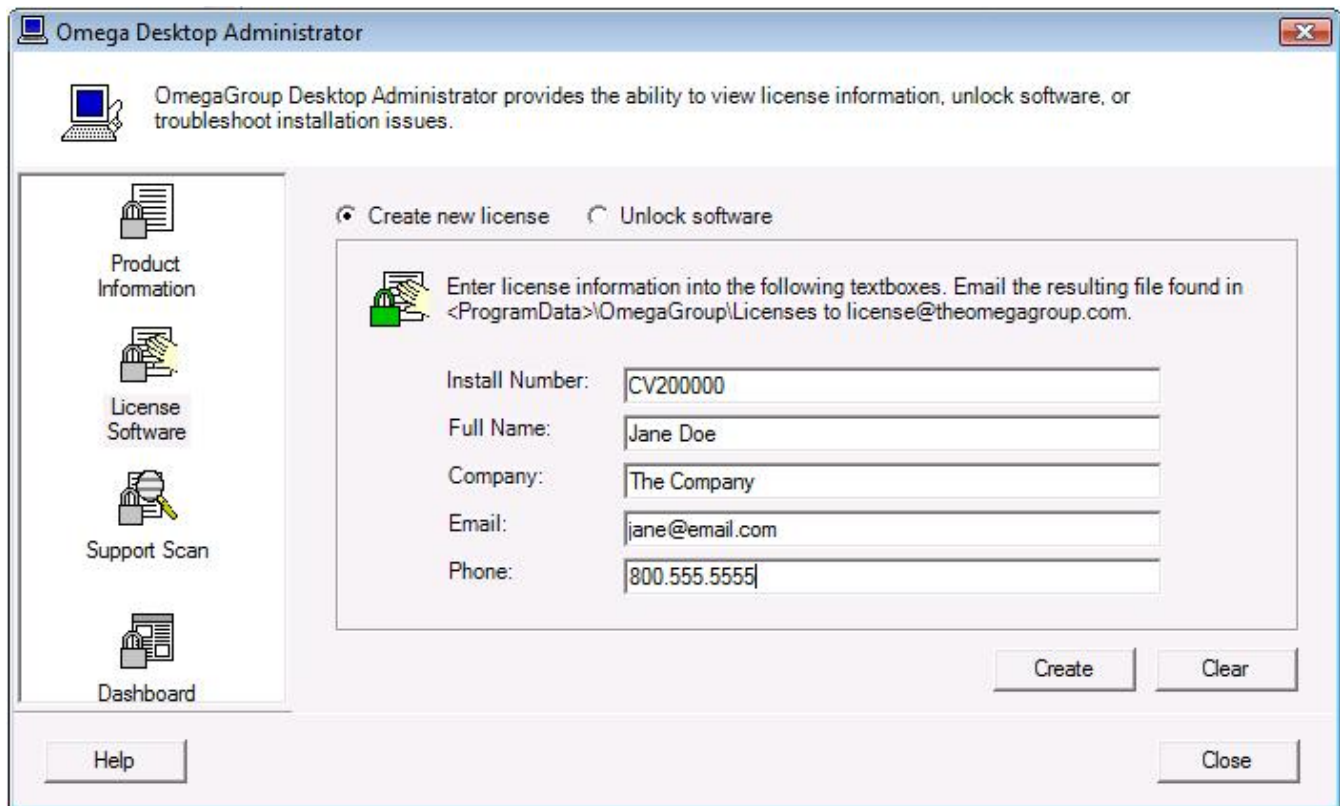
[Checking Available Licenses](#)

[Upgrading from a Previous Version](#)

Steps to License a Product

The Omega Desktop Administrator application is used to manage the licensing of all Omega Desktop products. This application was introduced in the Omega Desktop 4.0 release to replace the "License Manager" application.

- After the Omega Desktop software is installed, open the Omega Desktop Administrator. From the Windows "Start" button, navigate to the "Omega Group" -> "Desktop Administrator".
- With the application open, create a new license file. Navigate to the "License Software" view and ensure that the "Create New License" option is selected. Enter the required information.

Attachment A

When the information is entered, click the 'Create' button to generate the new license file. The license file is automatically saved to the <ProgramData folder>\OmegaGroup\Licenses folder. The new file name is a combination of the Install Number with the extension .ini.

- Email the new license file (ie CV2xxxxx.ini) to license@theomegroup.com. The license file is received by the staff at the Omega Group, updated in order to unlock the software, and returned to the client. The updated file name will be the same as the original file name but with a 'j' added to the end of the file (ie. CV2xxxxxJ.ini).
- Open the Omega Desktop Administrator, and navigate to the "License Software" view. Select the "Unlock Software" option, and browse to the location of the updated license file. If the software is unlocked successfully, the updated license file is copied to the <ProgramData folder>\OmegaGroup\Licenses folder.

Checking Available Licenses

Attachment A

There are two methods available to determine which Omega Desktop applications are licensed.

Omega Desktop Administrator

The Product License Information table in the Product Information view displays the software that is unlocked. To view the Product License table navigate to "Product Information" in the Omega Desktop Administrator. Software that has been licensed will be identified in the Product License Information list.

The Unlocked field identifies when the software was initially unlocked for use. The Expiration field is available if a temporary license has been created. If a temporary license is created, the expiration date will be listed.

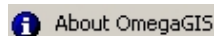


The screenshot shows the Omega Desktop Administrator window. The title bar reads "Omega Desktop Administrator". Below the title bar, there is a description: "OmegaGroup Desktop Administrator provides the ability to view license information, unlock software, or troubleshoot installation issues." On the left side, there is a navigation pane with a "Product Information" button. The main area displays a table titled "Product License Information".

Software	Install Number	Unlocked	Expiration	Valid
CrimeView	CV201230	01/31/2006	permanent	Valid
FireView	FV201237	01/27/2006	permanent	Valid
SchoolPlanner	SP202574	01/27/2006	permanent	Valid
ImportWizard	Iw201238	01/27/2006	permanent	Valid

About Omega Desktop

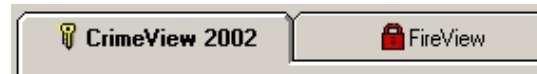
To determine which ArcMap extensions are enabled, use the "About Omega Desktop" dialog. To open this dialog, select "About Omega Desktop" item that is found on the CrimeView, FireView or School Planner pull-down.



This dialog has a tab for each extension. The tab has a key icon when the extension is licensed and a lock

Attachment A

icon when the extension is not licensed.

**Upgrading from a Previous Version**

If a previous version of Omega Desktop is installed and licensed, the upgrade to the latest version does not require updating the license.

Building An Application

Building a CrimeView application is a complex process that is unique for each client. Building the CrimeView application is typically a service provided by The Omega Group. This section highlights the major tasks when building the application.

[Retrieve Incident Data](#)

[Build Saved Queries](#)

[Build Crystal Reports](#)

[Set Default Fields](#)

[Create ArcMap Document](#)

[Create Map Templates](#)

Retrieve Incident Data

One of the first tasks in building a CrimeView project is retrieving the incident data. The incident data is used for analysis and provides the source data to create maps and reports.

The *Omega Import Wizard* provides a means to import datasets from Database Management Systems (DBMS) or ASCII text files. Once retrieved, the datasets are geocoded so that they may be used with OmegaGIS.

An Import Profile (*.oiw) is a file used by the Omega Import Wizard to outline the steps needed to retrieve and process the datasets. The Import Profile provides a processing template that records how to extract the dataset from the DBMS, which OmegaGIS fields to create, the geocoding steps involved and the final destination for the resulting feature class. Refer to the Omega Import Wizard documentation for further information.

Build Saved Queries

Attribute queries using SQL syntax to select features from incident datasets can often become lengthy and complex. [Saved Queries](#) hide the SQL syntax from the user while providing a more intuitive name or description for each query. Saved queries are created and edited with the [Saved Queries Editor](#) in ArcCatalog and are stored in the Omega_Query.MDB database.

Build Crystal Reports

CrimeView employs [Crystal Reports](#) for reporting functionality. Using the [OmegaGIS Metadata Editor](#), reports are registered to layers.

Set Default Fields

Using the [OmegaGIS Metadata Editor](#), set the default fields for the layers used by the CrimeView application. The default fields include:

- OmegaGIS Fields (date, day of week, time, response time).
- Incident Type for [graphs](#).
- Default field for list boxes in dialogs.

Create ArcMap Document

An ArcMap document containing incident datasets and other geography such as street centerlines provides the backdrop for performing geographic crime analysis. Every ArcMap document that uses OmegaGIS has an associated [project workspace](#) where the results of the routines and preferences are stored.

Attachment A

When creating the ArcMap document, the points outlined below should be followed:

- **All layers must have a unique name.**
Layer names in the table of contents are used by OmegaGIS routines for identification. If layers share the same name, the first layer in the stack is always used by OmegaGIS. If the name of the layer changes, Cyclical Reports or Threshold Alerts created with that layer, will no longer be able to recognize the source data, and an error will result. Consequently, it is important that all the layers are assigned a unique name in the table of contents, and retain their original names.
- **Data Frames must have a unique name.**
The name of the data frame is used with OmegaGIS routines. Consequently, the data frame names must be unique and should not change.
- **Use a projected coordinate system**
All layers and data frames should have a projected coordinate system (as opposed to a geographic coordinate system). This is not a requirement but it is recommended as a projected coordinate system will result in more accurate results.
- **Performance checklist**
The documentation contains a performance checklist that has recommendations for setting up an ArcMap document which should be followed.

Create Map Templates

[Map templates](#) are used to define how the map elements in the layout will appear. Map elements include a title, agency logo, legend, north arrow and scale bar. Map templates can be used with both [Cyclical Reports](#) and [Threshold Alerts](#).

Crystal Reports

Omega Desktop employs Crystal Reports for reporting functionality. Crystal Reports version XI, 11.5 and 12 are supported by Omega Desktop 4.3.2. The [Create Reports](#) utility enables the user to open reports created for OmegaGIS routines.

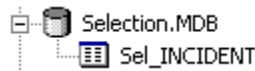
When building an application in CrimeView, FireView or School Planner there are several reports that should be generated or customized at the onset of the project. The following section describes these reports, many of which are provided as templates with the installation of OmegaGIS software, and can be customized to suit the project.

Reports Common to CrimeView, FireView and School Planner

- **Query Layer Reports**

[Query Layers](#) are common to all OmegaGIS Software products; CrimeView, FireView and School Planner. Query Layers are data layers based on point type geometry that identify the location of a particular data type. For instance, in the case of CrimeView, a Query Layer might identify where auto thefts have occurred whereas in School Planner, the Query Layer may represent where students live within the school district.

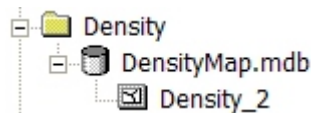
Query Layer Reports are based on the data of the Query Layer, and so must be created with the data in mind, and customized to each new project. Once created, the report must be registered to the Query Layer using the [OmegaGIS Metadata Editor](#). There is no limit to the number of Crystal Reports that can be registered to a Query Layer.



The 'Sel_INCIDENTS' table found in the Selection.MDB within the [project workspace](#), provides the source data for the Crystal Report that is based on a Query Layer.

- **Density Map Reports**

Density Map reports are created based on layers that are created by the [Density Map](#) routine. In order access the report, the boundary layer that is used to create the resulting density map layer, must have the name of the Density Map Report registered to it using the [OmegaGIS Metadata Editor](#). When the new map layer is generated, the [Create Reports](#) utility can be used to view the report associated with the new layer.



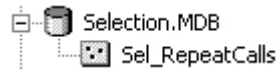
The source of the Density Map Crystal Report is the 'Density_*' feature class found in the [DensityMap.MDB](#), that is located in the Density folder of the [project workspace](#). A template for the Density Map Crystal Report is located in <Installation Directory>\OmegaGroup\Desktop\Reports\Template_DensityMap.rpt.

- **Repeat Calls (Student Concentrations)**

The [Repeat Calls](#) routine (Student Concentrations in School Planner) creates a layer that reveals the places that have numerous incidents (students) at the same location. The Repeat Calls (Student Concentrations) report summarizes the incidents (students) found at the same locations. The [Query Layer](#) that was used to generate the Repeat Calls (Student Concentrations) layer must have a Repeat Calls (Student Concentrations) Crystal Report

Attachment A

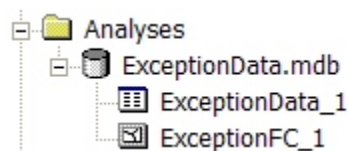
registered to the layer using the [OmegaGIS Metadata Editor](#).



The 'Sel_RepeatCalls' table, found in the Selection.MDB within the [project workspace](#), provides the source data for the Crystal Report. A text field named "OmegaGIS_XY" in the 'Sel_RepeatCalls' table can be used to group the incidents (students).

- **Exception Reporting (Enrollment Comparison)**

The result of the [Exception Reporting](#) (Enrollment Comparison in School Planner) routine is both a layer and a Crystal Report. The report is named Exception.RPT and is located in the <Installation Directory>\OmegaGroup\Desktop\Reports folder. The source table for the report is "ExceptionData_*" which is located in the \Analyses\ExceptionData.MDB personal Geodatabase in the [project workspace](#).



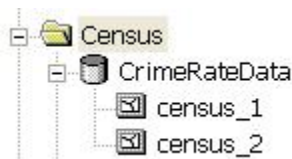
The Exception.RPT may be customized, such as adding an image to the report, but the report must have the original name. The report can be located in a location other than the default \reports folder within the project directory, however, the folder location must be referenced using the Locations category for Crystal Reports in Setup. The original fields found on the Exception Report should not be modified as they are based on standardized output created when the Exception Report routine is run.

CrimeView Reports

- **Crime Rate Generator**

Three report templates are provided with Crime Rate Generator and are found in the <installation folder>\OmegaGroup\Desktop\Reports folder. When a Crime Rate Generator routine is run, and the 'Report' option is selected on the dialog, the report template is copied to the [project workspace](#) \Reports folder and is used to view the Crime Rate Generator results.

Each report is related to a specific census layer that is generated with the OmegaGIS Demographic Data Loader. When the census layer is created a metadata tag is created automatically to ensure that the correct report is used with the layer. For instance, the CrimeRate_Block.rpt report is used with the census blocks layer, the CrimeRate_Blockgroup.rpt report is associated with the blockgroup layer and the CrimeRate_Tract.rpt is used with the census tract layer.



When the Crime Rate Generator analysis is run, a new feature class is created in a personal geodatabase called CrimeRateData.mdb located in the project \Census folder. Each new

Attachment A

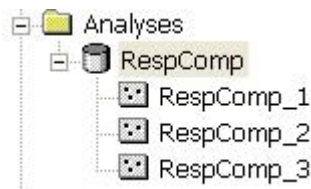
feature class is numbered chronologically and prefixed with 'census_'. The report can be customized in order to change the format, however the original fields on which the report is based should not be altered as they reference standardized data output created by the routine.

FireView Reports

- **Response Comparison Analysis**

The Response Comparison Analysis report (RespComp.rpt) is a template provided with OmegaGIS. It is found in the <installation folder>\OmegaGroup\Desktop\Reports folder of the project workspace. The Response Comparison Report is based on the Omega_Difference field in the results layer, and defines the difference in time between the actual arrival time of equipment to an incident, and the expected time calculated using the OmegaGIS Street Network Manager.

The Response Comparison report can be customized, renamed and located in any folder. To enable the Response Comparison report, the query layer on which the response analysis is based, must have a metadata tag attached to it that references the name of the Response Comparison report. Setting this tag can be accomplished with the [OmegaGIS Metadata Editor](#). If the report is not placed in the default [project workspace](#) \Reports folder, the Locations category of Setup must reference the new folder. Although, the content of the report can be customized, the original fields of the report should remain as they are based on standardized fields that are available with the analysis.



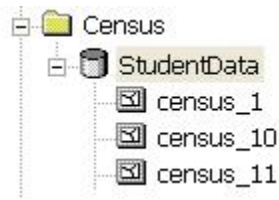
Response Comparison feature classes generated by the routine are stored in a personal geodatabase called RespComp.mdb in the project \Analyses folder. Within the database, each feature class created is chronologically named using the prefix 'RespComp_' and an attached number.

School Planner Reports

- **Demographic Analysis**

Three report templates are provided with Demographic Analysis and are found in the <installation folder>\OmegaGroup\Desktop\Reports folder. When a Demographic Analysis routine is run, and the 'Report' option is selected on the dialog, the report template is copied to the [project workspace](#) \Reports folder and is used to view the Demographic Analysis results.

Each report is related to a specific census layer that is generated with the OmegaGIS Demographic Data Loader. When the census layer is created a metadata tag is created automatically to ensure that the correct report is used with the layer. For instance, the Student_Block.rpt report is used with the census blocks layer, the Student_Blockgroup.rpt report is associated with the blockgroup layer and the Student_Tract.rpt is used with the census tract layer.

Attachment A

When the Demographic Analysis routine is run, a new feature class is created in a personal geodatabase called StudentData.mdb located in the project \Census folder. Each new feature class is numbered chronologically and prefixed with 'census_'. The report can be customized in order to change the format, however the original fields on which the report is based should not be altered as they reference standardized data output created by the routine.

- **Projection Analysis (Attending and Residing)**

There are two reports associated with Projection Analysis; the Residing report and the Attending report. Both reports are provided as templates in the <installation folder>\OmegaGroup\Desktop\Reports folder, and are called Template_Residing.rpt and Template_Attending.rpt.

These reports can be customized, renamed and stored in any accessible folder. If these reports are stored anywhere but the default \reports folder however, the folder location must be referenced by Setup under the Locations category for Crystal Reports. The reports must also be registered to the data layers on which the analysis is performed. For instance, each student layer used in the analysis should have the Residing and Attending report names registered to them using the [OmegaGIS Metadata Editor](#).



The data on which the Residing and Attending reports are based is stored in a personal geodatabase called Omega_Projection.mdb within the project \Analyses folder. When a Projection Analysis is run a new feature class (fclass_*) and a new table (scenario_*) are generated. Both data items are numbered chronologically. It is the scenario table that houses the data on which the reports are based.

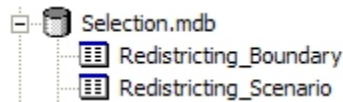
- **Boundary Redistricting**

[Boundary Redistricting](#) supports two reports; a boundary report and a scenario report. The [Boundary Report](#) displays a summary of the students that have been assigned to the school selected in the Facility list. The [Scenario Report](#) displays a summary of the number of assigned students to all of the school boundaries of the current scenario.

Both reports are provided as templates in the <installation folder>\OmegaGroup\Desktop\Reports folder and are called Redistricting_Boundary.rpt and Redistricting_Scenario.rpt respectively. These reports may be customized, renamed and stored in any folder, as long as that folder is referenced by the Locations category for Crystal Reports in Setup. The reports must also be registered to the query layers on which they are based using the [OmegaGIS Metadata Editor](#).

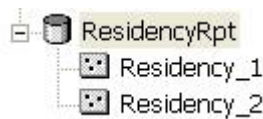
Attachment A

The source tables for the reports are located in the Selection.MDB that is located in the project workspace.



- **Residency Report**

The Residency Report is associated with a report that is distributed as a template in the <installation folder>\OmegaGroup\Desktop\Reports folder. The report is called Template_Resident.rpt and includes both a summary and detailed section. The report can be customized, renamed and relocated, however the location of the report must be referenced by the Locations Category for Crystal Reports in Setup, and the report must be registered to the query layer using the [OmegaGIS Metadata Editor](#).



The source data on which the report is based is stored in a personal geodatabase within the project \Analyses folder. The database is called ResidencyRpt.mdb. When a residency analysis is run, the resulting data is stored in a new feature class called Residency_* where the * represents a number that increases each time a new residency report is generated.

Project Workspace

An OmegaGIS project, such as CrimeView, is set up in an ArcMap document. Every project has an associated *project workspace* that is used to store the results of routines and preferences. This section describes the project workspace.

[Name of Project Workspace](#)

[File Structure](#)

Name of Project Workspace

The project workspace is a folder that has the same name as the ArcMap document. For example, if the ArcMap document is named MyMap.MXD and is located in the C:\CrimeView folder, then the project workspace is C:\CrimeView\MyMap.

File Structure

The files and folders that are automatically generated in the project workspace are outlined below:






MyMap.MXD

MyMap






The project workspace has the same name as the ArcMap document without the file extension.

Analyses

The Analyses folder is always created by OmegaGIS routines. The folder may contain a number of personal geodatabases depending on the Omega software product in use.



-  *AddQueryLayers.MDB (common to all Omega products)*
When [additional query layers](#) are used in any of the OmegaGIS software products, the incidents selected by the attribute query and/or spatial query, are exported into the same feature class in this personal Geodatabase. The AddQueryLayers.MDB is created dynamically, if it is not present it is created automatically.
-  *ExceptionData.MDB (common to all Omega products)*
This personal Geodatabase is used with the [Exception Reporting](#) routine. It is created when the routine is run. If the database is deleted, it is regenerated automatically.
-  *ResponseAnalysis.MDB (FireView)*
This personal Geodatabase is used with the Response Analysis routines, such as [First Due](#). It is created when the routine is run, and is regenerated automatically if deleted.
-  *AvgRespTime.MDB (FireView)*
This personal Geodatabase is used with FireView's [Response Time Map](#) routine and is created when the routine is run. If the database is deleted, it is recreated automatically.
-  *RespComp.MDB (FireView)*
During the [Response Comparison](#) routine in FireView, a new feature class is generated in the RespComp.MDB personal Geodatabase. This file is created when the routine is run, and is regenerated automatically if deleted.

Attachment A

-  **StatProfiler.MDB (CrimeView, FireView)**
This personal Geodatabase is used with the [Statistical Profiler](#) routine and is created when the routine is run. The database is regenerated automatically if deleted.
-  **StnAnalyses (FireView)**
The StnAnalyses folder is created by FireView's [Station Analysis](#) routine and contains the ProposedStations.MDB personal Geodatabase.
-  **Omega_Projection.MDB (School Planner)**
During the Projection Analysis routine in School Planner, a new feature class and scenario table are generated in the Omega_Projection.MDB personal Geodatabase. The geodatabase is created when the routine is run, and is regenerated automatically if deleted.
-  **Redistrict.MDB (School Planner)**
During the [Boundary Redistricting](#) routine in School Planner, a number of tables and feature classes are generated in the Redistrict.MDB personal Geodatabase. The geodatabase is created when the routine is run, and is regenerated automatically if deleted.
-  **ResidencyRpt.MDB (School Planner)**
During the Residency Report routine in School Planner, feature classes are generated in the ResidencyRpt.MDB personal Geodatabase. The geodatabase is created when the routine is run, and is regenerated automatically if deleted.

 **Density**

The Density folder is always created by OmegaGIS routines. The folder may contain two personal Geodatabases:


-  **DensityMap.MDB (common to all Omega products)**
During the [Density Map](#) routine, a new feature class is generated in the DensityMap.MBD. The DensityMap.MDB file is created automatically while running the Density Map routine.
-  **RepeatCalls.MDB (common to all Omega products)**
The RepeatCalls.MDB file is created during the [Repeat Calls](#) routine (Student Concentration routine in School Planner). It contains the feature class that has the repeat locations.

 **HotSpot**

The HotSpot folder contains the rasters from the [Hot Spot](#) routine (Spatial Clustering in School Planner) and is always created by OmegaGIS routines. The rasters are temporary and are automatically deleted from disk when they are no longer referenced by ArcMap. This folder is common to all Omega products.



 **Census**

The Census folder is always created by OmegaGIS routines. The folder may contain up to three personal Geodatabases:





-  **CrimeRateData.MDB (CrimeView)**
During the [Crime Rate Generator](#) routine, a new feature class is generated in the CrimeRateData.MDB personal Geodatabase. The CrimeRateData.MDB file is created automatically while running the Crime

Attachment A





Rate Generator routine.

-  **StudentData.MDB (School Planner)**
During the Demographic Analysis routine, a new feature class is generated in the StudentData.MDB personal Geodatabase. The StudentData.MDB file is created automatically while running the Demographic Analysis routine.
-  **Omega_DemoViewer.MDB (common to all Omega products)**
During the [Demographic Viewer](#) routine, a new feature class is generated in the Omega_DemoViewer.MDB personal Geodatabase. The Omega_DemoViewer.MDB file is created automatically while running the Demographic Viewer.

The Census folder may also contain the personal Geodatabase that has the census feature classes.

-  **Selection.MDB**
The Selection.MDB personal Geodatabase is automatically created by OmegaGIS routines if not already present. It is used to store selected records that OmegaGIS [graphs](#) and [Crystal Reports](#) use as a source.
-  **Setup.MDB**
The Setup.MDB file contains user defined preferences for the ArcMap document. There is a password on the Setup.MDB file. The only way to alter the preferences is with the [OmegaGIS Setup](#) dialog.
-  **Threshold_Alert.MDB**
Cyclical Reports and Threshold Alerts are stored within the Threshold_Alert.MDB database.
-  **MyMap.XML**
The XML document has the same name as the ArcMap document and contains information on the last routine run. The document is created when a routine is run.

Other folders and files can be included in the project workspace. The other folders and files that typically make up the project workspace include the following:

-  **Geography**
This folder contains the geographic datasets used with the OmegaGIS routines. Examples of geographic datasets include Police Beats, School Districts and street centerlines.
-  **Reports**
The Reports folder in the project workspace is the default search location for Crystal Reports. Search locations can be changed by using the [OmegaGIS Setup](#) dialog.
-  **Network**
This folder in the project workspace is the default search locator for [Omega Street Network](#) folders which are used with FireView. Search locations can be changed by using the [OmegaGIS Setup](#) dialog.
-  **Omega_Query.ODB**
The Omega_Query.ODB file contains the Saved Queries. The default location is in the

Attachment A

project workspace. This location can be changed by using the [OmegaGIS Setup](#) dialog. In versions of OmegaGIS prior to Omega Desktop 4.0, this database was named Omega_Query.MDB (note the extension). This database can be updated from a previous version using the Omega Query Editor tool on the Omega Data Manager toolbar in ArcCatalog.

Map Templates

In ArcMap, the layout contains all of the elements of a map. These map elements may include a title, agency logo, legend, north arrow, scale bar and geographic layers. These map elements can be organized so that all maps, whether printed or created as an image, that are produced with ArcMap share a similar professional design.

One way to change the layout appearance of a map is to use the tools in ArcMap to insert new map elements, such as a north arrow. Once added, map elements can be moved by clicking on the element and dragging it to a new location. Another way to change the appearance of the layout is to use a *map template*. A map template contains these map elements so that there is no need to spend time creating a map.

This help section outlines the following:

- [Use of Map Templates](#)
- [Creating a Map Template](#)
- [Map Template Considerations](#)

Use of Map Templates

When using Omega GIS products, such as FireView, map templates can be used with the following:

- **Layout**

The map layout can be quickly changed by loading a map template using the Change Layout tool available in ArcMap. This tool is on the Layout toolbar and is also available on the CrimeView/FireView pull-down menu.



The Change Layout tool opens a dialog that allows one to browse to an existing template. Click the Browse button and navigate to an existing map template (.MXT).

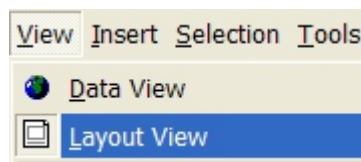
- **Cyclical Reports and Threshold Alerts**

Both [Cyclical Reports](#) and [Threshold Alerts](#) support the use of map templates. When a map template is used, the map template is automatically loaded when the routine is completed.

Creating a Map Template

The following steps outline how to generate a map template:

1. Make the layout view the active view in ArcMap. From the View pull-down menu item select Layout View.



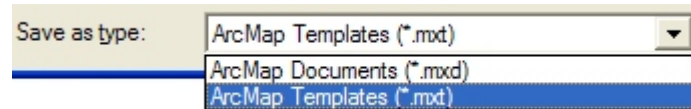
Tip: Another way to make the layout view active is to select the layout view button located at the bottom left hand side of the data view.

Attachment A

2. With the layout view active, insert and arrange map elements. To insert map elements, such as a north arrow, from the Insert pull-down menu select the map element to insert.

To remove all the map elements but the data frame, use the [Remove Layout Elements](#) tool.

3. Once the map elements on the layout have been arranged, the next step is to save these changes as a map template. From the File pull-down menu select Save As which opens a new dialog. Change the save type from an MXD (ArcMap Document) to an MXT (ArcMap Template) and then provide a location and file name.



Once the document has been saved as a Template, the current ArcMap document provides the template. Any changes to the map elements on the layout are saved to the template.

Since Omega GIS routines require that ArcMap is not a template an error message [6700111] is issued when a dialog is opened. To return to the ArcMap document, from the File pull-down menu select Open and then navigate to the MXD.

Map Template Considerations

When using map templates with Omega GIS products, such as CrimeView, there are some considerations to be aware of:

- **Pictures in Layout**

When inserting pictures into the layout, such as an agency logo, save the picture as part of the document. Right click the picture and select Properties from the pop-up menu. On the Picture tab, check the Save Picture as Part of Document.



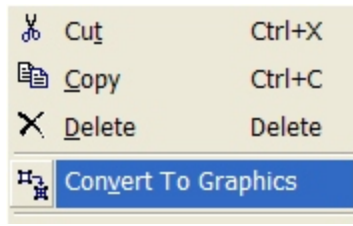
When the picture is not saved as part of the document, ArcMap must reference the picture on disk. If the pictures disk location is altered then an error message is issued every time the ArcMap document is opened.

- **Legends**

Omega GIS query routines, such as Incidents Within A Boundary, create a new selection layer based on the results of the routine. Unfortunately, these legends do not work well with map templates and it is recommend that the legends not be stored in the map template.

One solution is to insert the legend and then convert the legend to graphics which prevents the legend from dynamically changing when items in the table of contents are altered. To convert the legend, right click the legend in the layout and then select Convert to Graphics from the pop up menu.

Attachment A



Upgrading from previous versions

Upgrading from previous versions of OmegaGIS to Omega Desktop 4.3 requires three procedures in order to ensure that the analyses and tools provided with the software operate correctly.

Omega Query Database

At the Omega Desktop 4.2 release, the Omega Query Database format was revised in order to provide greater functionality when building Saved Queries, as well as accommodate new data formats issued with ArcGIS 9.0. The 4.0 version of the query database was named Omega_Query.ODB instead of Omega_Query.MDB. This version of the database persists in the Omega Desktop 4.2 version of the software.

If upgrading from a version of the Omega Desktop software, prior to 4.0, the Omega_Query.mdb can be upgraded using a tool provided within the [Omega Query Editor](#). The tool gives the user the ability to select the old database, and automatically convert the database format and the data within to the new version. The Omega Query Editor is available on the Omega Data Manager Extension to ArcCatalog.

Import Wizard

At the Omega Desktop version 4.0 release, the Omega Desktop installation was created as a single CD that includes all Omega Desktop products. All of these products are installed and the use of the products is controlled by the licensing.

One of the changes brought about by this installation is that the Omega Import Wizard program files have changed location in the installation directory. The automation of the Omega Import Wizard uses the path of the OmegaWizard.EXE file in the Windows Task Scheduler. This path change been change to <Installation directory>\OmegaGroup\Desktop\Bin.

Existing Window Task Scheduler task must be updated to use the new path to the OmegaWizard.EXE.

Threshold Alerts

The Windows Task Scheduler may be used to automate [Threshold Alerts](#). This is done by setting up a task that provides the path to the ThresholdAuto.EXE and the ArcMap document. The folders that contain the Omega Desktop software have changed as of the version 4.0 release; including the path to the ThresholdAuto.EXE.

The path to the ThresholdAuto.EXE has been changed to <Installation directory>\OmegaGroup\Desktop\Bin.

Existing Window Task Scheduler task must be updated to use the new path to the ThresholdAuto.EXE.

Upgrades Prior to Service Pack 2

The following information applies only to those situations where an upgrade is made from an OmegaGIS release prior to Service Pack 2. Service Pack 2 and subsequent releases, include a number of new features that require making some updates to existing CrimeView applications. This section highlights the issues faced when upgrading from a version of CrimeView that was installed prior to Service Pack 2.

Attachment A

[Licensing](#)
[Normal.MXT](#)
[Extension and Toolbar](#)
[Cyclical Reports](#)
[Repeat Calls](#)
[Legacy Files](#)

Licensing

CrimeView software that has been licensed prior to Service Pack 2 does not require updating. The license information is retained as long as the previous version of the software is not uninstalled prior to installing the new version.

Normal.MXT

If CrimeView was installed prior to Service Pack 2, and is upgraded the *hot-key* to run the Clear All, F11, will not work. A hot-key is a shortcut to a tool from the keyboard. This is a known issue with ArcMap.

The current work around to this issue is to delete the existing Normal.MXT. The Normal.MXT stores information on which toolbars are used in all ArcMap documents and is unique for each user that logs into the machine. The location of the Normal.MXT is in the \Documents and Settings\
Current User >\Application Data\ESRI\ArcMap\Templates folder. Close ArcMap and then delete the existing Normal.MXT, the file will be generated once ArcMap is opened.

If the Normal.MXT is not deleted, the Clear All can still be run from the OmegaGIS toolbar by clicking the Clear All button.



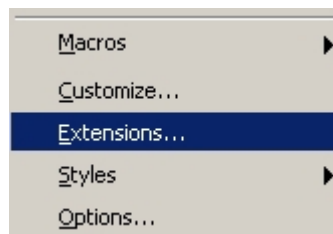
When the hot-key is working correctly, the OmegaGIS Step item on the CrimeView pull-down menu will have F11, otherwise the menu item will not have any hot-key information.

Extension and Toolbar

The OmegaGIS extension must be enabled and the toolbar must be added to ArcMap after the upgrade to Service Pack 2.

Enable Extension

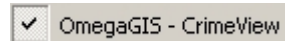
From the Tools pull-down menu in ArcMap, select Extensions to open the Extensions dialog. Check the "CrimeView" extension and close the dialog. A message is issued if the extension is not [licensed](#) correctly.



Information on which extensions are enabled is based on the current user logged into the machine, and is stored in the computers registry (HKEY_CURRENT_USER). All new or existing ArcMap documents have the CrimeView extension enabled. If a different user logs into the machine, the CrimeView extension must be enabled.

Attachment A**Add Toolbar**

To add the CrimeView toolbar, from the View pull-down menu in ArcMap, select Toolbars and then check the "OmegaGIS - CrimeView" item.



Once added to ArcMap, the CrimeView toolbar is available to all ArcMap documents for the current user. Information on which toolbars are in use for all ArcMap documents is stored in the Normal.MXT. As the Normal.MXT is stored in the \Documents and Settings\

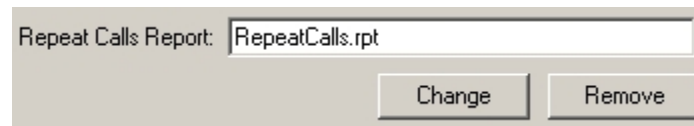
Cyclical Reports

[Cyclical Reports](#) built with a previous versions of CrimeView are not supported by Service Pack 2 or subsequent releases. This change is a result of accommodating the use of Threshold Alerts.

Consequently, all Cyclical Reports must be built again with Service Pack 2 or subsequent releases.

Repeat Calls

At Service Pack 2 and beyond, Query Layers that are used to generate Repeat Calls layers must have a [Repeat Calls Report](#) registered to it. In previous versions, only one Repeat Calls Report was supported which limited the report to one dataset. To register a Repeat Calls Report, use the OmegaGIS Metadata Editor that is found in ArcCatalog.



The Repeat Calls Report uses the Sel_RepeatCalls table in the Selection.MDB file as the source for the Crystal Report. The Sel_RepeatCalls table has a field called "OmegaGIS_XY". The values in this field can be grouped in Crystal Reports to determine the repeat call location. The "OmegaGIS_XY" field was named "CV_XY" in previous versions of OmegaGIS, consequently, existing Repeat Call Reports must be updated to use the new field name.

IWdate	OmegaGIS_XY
20030103	923586.291 866687.058
20030103	923635.571 866645.967

Legacy Files

At Service Pack 2, the [project workspace](#) is reorganized. Consequently, there are legacy files and folders that can be safely removed from the project workspace as they are no longer used. Below is a list of folders and files that can be removed:

**Connectivity**

The Connectivity folder is not used by any OmegaGIS routine.

**Grid**

The Grid folder is not used by any OmegaGIS routine.

**Repeat**

Attachment A

The Repeat Calls routine at Service Pack 2 uses the Density folder.

**Cyclical.MDB**

[Cyclical Reports](#) built with previous versions of CrimeView are not supported at Service Pack 2. The Cyclical.MDB file was used to store the Cyclical Reports, now the information is stored in the Threshold_Alert.MDB file.

**Omega_QDSum.XSL**

The stylesheet used with the summary dialog has been moved to the Windows TEMP directory.

**QDSummary.HTM**

This file contained information on the last routine run in HTML format. The information is now available with the Layout Metadata tool.

**QDSummary.TXT**

This file contained information on the last routine run in a text format. The information is now available with the Layout Metadata tool.

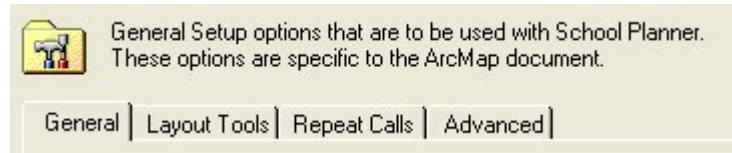
**TOC.HTML**

This file is no longer in use.

Setup: General

The General Category in Setup contains generic settings that affect the ArcMap document, the Layout, and Omega Desktop routines. The General Settings are subdivided into three subcategories that represent tabs in the Setup Dialog. These subcategories are:

[General](#)
[Layout Tools](#)
[Repeat Calls](#)
[Advanced](#)



General

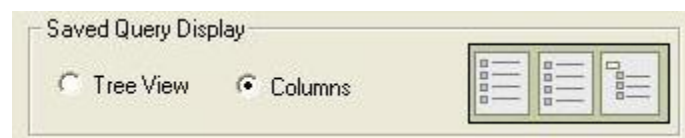
Measurement System

The two choices for Measurement System are English and Metric, where English is the default setting. The English system employs feet and miles, whereas the Metric system employs meters and kilometers

This setting alters appropriate OmegaGIS dialogs regarding measurement, such as default buffer units. This setting does not alter the Data Frame's map units and distance units, which can be set by selecting the Data Frame Properties option from the View menu.

Saved Query Display

Saved queries can be displayed within analysis dialogs in tree view or in column view. The tree view presents the saved queries in a hierarchical structure. The column view has three columns, where the first two are populated by the child queries of a Level 1 query, and the third column shows the remaining saved queries in a hierarchical structure. The Omega Query Editor is used to set which queries will be displayed in the first two columns.



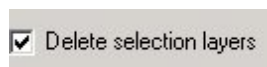
Upon Project Exit

Project exit settings are executed when the ArcMap document is closed. To apply the settings immediately without closing the ArcMap Document click the Apply Project Exit button.



- **Delete Selection Layers**

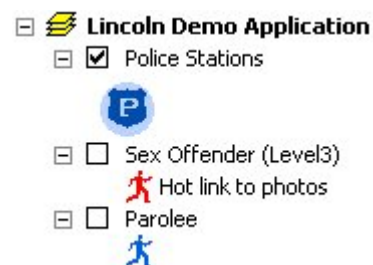
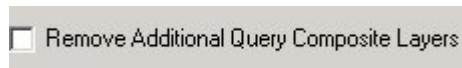
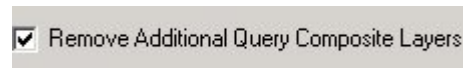
This setting when checked specifies that all selection layers will be removed from the ArcMap document when closed. The default is to delete the selection layers.



Attachment A

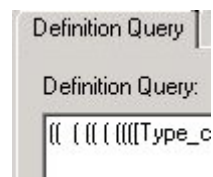
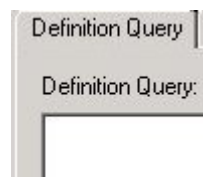
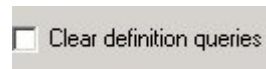
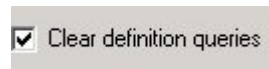
- **Remove additional Query Composite Layers**

When this box is checked, all [composite layers](#) will be removed from the ArcMap document when closed. The default is to delete the composite layers.



- **Clear Definition Queries**

When this box is checked, all [Omega Definition Queries](#) will be removed all the layers when the ArcMap document is closed. The default is to clear the query definitions.



Layout Tools

The text entered for the Layout Tools updates the disclaimer used in the [Layout Metadata Tool](#). The text is limited in length to 255 characters. The default for this setting is as follows:

This agency is not responsible for the misinterpretation of this map and makes no inference or judgment as to the relative safety of particular areas. This map does not meet national map accuracy standards and should not be used for engineering purposes.

Repeat Calls

Attachment A**Report Buffer Distance**

When the repeat calls report is created, the records from the source Query Layer are exported to the Selection.MDB located in the project workspace. A spatial filter is used to select the records in the Query Layer to include in the export. This spatial filter uses the attribute query that was used to generate the Repeat Calls layer, if any, and the geometry of the repeat calls locations. The geometry of the repeat calls locations is buffered before being placed in the spatial filter and the Report Buffer Distance controls the size of the buffer.

The buffer distance is measured in meters and there is a default value of 0.5 m.

Advanced**Date Ranges**

Date range settings are used with the [Date and Time Query](#) dialog that is typically located on the **When?** tab of Query, Density, and some Analysis routines. The calendars display the available date range in white, while those dates that are unavailable are grayed out. Unavailable dates cannot be selected.

- **Display the available ranges of dates for the query layer**

When this option is checked, the metadata for selected Query Layers will be searched to get the date range information. The date range information is created by the Omega Import Wizard and specifies the beginning date, the ending date, and the OmegaGIS date field. The default is to display the available ranges of dates for the query layers.

- **Search query layer's feature class for date range when missing metadata information**

When this option is checked and the date range is not found in the metadata, the feature class will be searched to get the date range information. To accomplish this, each record in the feature class must be examined to determine the beginning date and ending date.

The searching of the feature class may result in a performance hit, especially if the feature class contains a large number of records. The field searched will be the default OmegaGIS date field. In an effort to improve performance, the default setting will not search the query layer's feature class for date range when missing metadata information.

For more information about date ranges see [Available Date Range for Query Layer](#).

Unique Lists

One method to select features in the boundary layer is "By Field Value", which requires a unique list of values. Many OmegaGIS routines use a boundary layer to query incidents geographically. This information is typically gathered on the **Where?** Tab of OmegaGIS routines.

- **Number of records used to determine list of unique values:**

When the boundary layer and field are selected, a list of unique values is generated based on the selected field. This unique set of values is then displayed in the [Field Values list](#). To populate this list each record in the feature class must be examined. In order to improve performance, this setting limits the number of records that are searched to generate a unique list. Therefore, if a feature class contains 100,000 records and this setting is set to 1,000, only the first 1,000 records will be cycled through to determine the values for the unique list. The maximum number of records used to generate a unique list is 10,000. To override this setting while executing a routine click the Complete List button. This will cycle through all

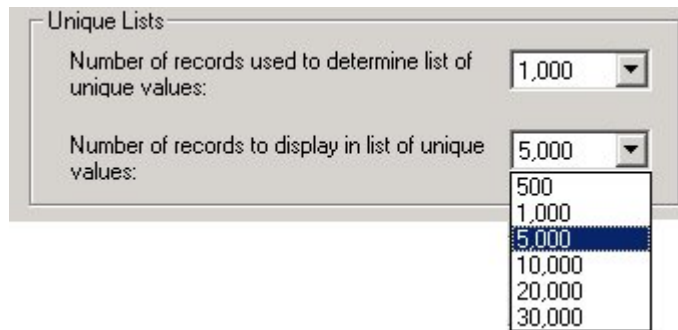
Attachment A

records in the feature class regardless of this setting. The default for this setting is 1,000.



- **Number of records to display in list of unique values:**

This setting limits the number of unique values displayed in the Field Values list. If a feature class has 10,000 unique values and this setting is set to 5,000, only the first 5,000 unique values will be displayed in the list. When the limit of unique values is reached, a warning is displayed to the left of the list. The maximum number of unique values that can be displayed in the Field Values list is 30,000. If this becomes an issue, use the [By Pointing](#) selection method. The default for this setting is 5,000.



Thumbnail

- **Save thumbnail image in metadata when ArcMap closes (not recommended)**

This tool is analogous to the Save thumbnail image with map check box on the map properties dialog in ArcMap. This setting could result in a performance hit when saving the ArcMap document, therefore the default does not save the thumbnail image.

Default Settings Buttons

The default setup values are stored in the template Setup.mdb database located in the install directory. Initially default Omega setup values are populated in the template Setup.mdb database.

These values can be found in the table below and are also included in each setting topic in the help.

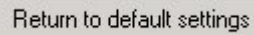
Attachment A

Setting	Value
Measurement System	English
Delete Selection Layers	<input checked="" type="checkbox"/>
Remove Additional Query Composite Layers	<input checked="" type="checkbox"/>
Clear Definition Queries	<input checked="" type="checkbox"/>
Layout Tools	<see Help topic>
Display the available ranges of dates for the query	<input checked="" type="checkbox"/>
Search query layer's feature class for date range when missing metadata information	<input type="checkbox"/>
Number of records used to determine list of unique values:	1000
Number of records to display in list of unique values:	5000
Save thumbnail image in metadata when ArcMap closes (not recommended)	<input type="checkbox"/>
Show all values and highlight only the selection	<input type="checkbox"/>
Show only saved query values and highlight selection	<input type="checkbox"/>
Show only selection (as new layer)	<input checked="" type="checkbox"/>
Allow only one selection layer	<input checked="" type="checkbox"/>
Create a legend for new layer with only selected	<input checked="" type="checkbox"/>
Display the routine summary dialog	<input checked="" type="checkbox"/>
Shrink the OmegaGIS dialog when routine is complete	<input checked="" type="checkbox"/>
Zoom to selection	<input checked="" type="checkbox"/>
Only use registered layers to make new queries	<input type="checkbox"/>
Create the 'OmegaGIS_Source' field that records the name of the source layer	<input checked="" type="checkbox"/>
Only create one new composite layer from each master query layer	<input checked="" type="checkbox"/>
New layer added by OmegaGIS routine is selectable	<input type="checkbox"/>
Exclude layers created from OmegaGIS routines from being used in new queries	<input checked="" type="checkbox"/>
Select features used as boundaries, such as 'Police Beats', that are used with OmegaGIS routines	<input checked="" type="checkbox"/>
Clear selection on registered query layers.	<input checked="" type="checkbox"/>
Remove additional query composite layers.	<input checked="" type="checkbox"/>
Remove OmegaGIS graphics, labels, and buffers.	<input checked="" type="checkbox"/>
Remove selection layers.	<input type="checkbox"/>
Turn off visibility of selection layers	<input checked="" type="checkbox"/>
Turn off visibility of registered query layers.	<input checked="" type="checkbox"/>
Turn off visibility of layers that are registered as 'Other'.	<input checked="" type="checkbox"/>
Zoom to:	<input type="checkbox"/> Home
Label Style:	Use layer label
Near an address label style:	Buffer Balloon Callout
Add labels to a new feature linked annotation group	<input checked="" type="checkbox"/>
Weight of new annotation group:	High
Weight of default annotation group:	High
Weight of OmegaGIS buffer annotation group:	Medium
Splash Screen displayed on startup	<input checked="" type="checkbox"/>
The OmegaGIS Tab in the ArcMap Table of Contents is shown when an OmegaGIS extension is enabled	<input checked="" type="checkbox"/>
The OmegaGIS Tab will display the number of selected features in the list with the layer name	<input checked="" type="checkbox"/>
All extensions used with OmegaGIS routines (ie. Spatial Analyst) will be automatically	<input checked="" type="checkbox"/>

Attachment A

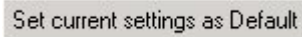
- **Return to default settings**

This button replaces the current settings from the entire setup database with the values saved in the template setup database. If the template setup database has not been modified by the Set current settings as Default button, then the setup values will return to the Omega default values. If the template has been modified, the setup values will be set to the modified values.

A rectangular button with a light gray background and a thin black border. The text "Return to default settings" is centered in a dark gray font.

- **Set current settings as Default**

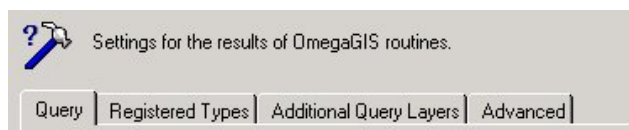
This button takes all the current settings for the entire setup database and saves them to the template setup database. This tool can be used to override the default settings that Omega provides. Setting the template with amended values insures that all newly created OmegaGIS projects will use the current setup values as their defaults. It also allows the user to store amended default settings for reuse later by using the Return to default settings button.

A rectangular button with a light gray background and a thin black border. The text "Set current settings as Default" is centered in a dark gray font.

Setup: Queries

The Query category in Setup contains settings that affect the input of data into OmegaGIS routines as well as the output from these routines. The Query Settings are subdivided into four subcategories that represent tabs in the Setup Dialog. These subcategories are:

[Query](#)
[Registered Types](#)
[Additional Query Layers](#)
[Advanced](#)



Query

The Query tab includes several options for how the results of an OmegaGIS routine will be displayed.

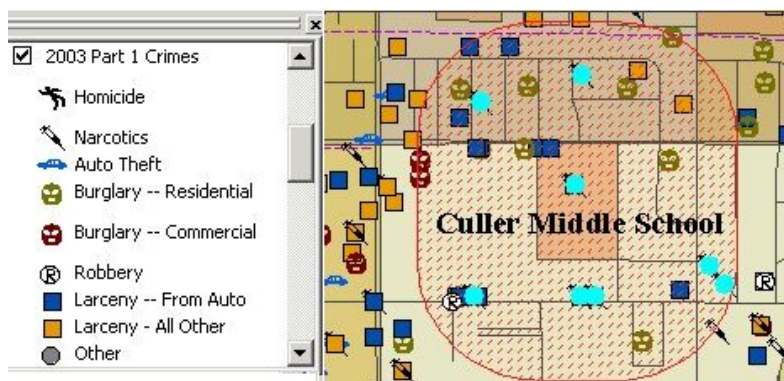
Select one of the following for the query results:

[OmegaGIS query routines](#) use attribute and geographic queries to identify the particular incidents in the [Query Layer](#). Attribute queries are based on the data stored in the table of Query Layer. For example, you might choose to display only those incidents that involved Narcotics. This data is specified on the **What?** and the **When?** tabs. Geographic queries are based on the spatial relationship of the Query Layer with other layers in the map. For example, you might want to see the Incidents that occurred within 1,000 feet of a school. This data is specified on the **Where?** Tab.

This setting will by default create a new selection layer for each OmegaGIS routine run.

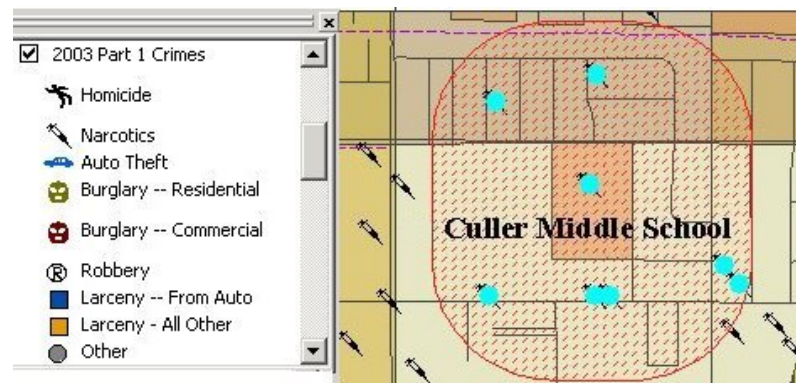
- **Show all values and highlight only the selection**

This option will select the incidents in the Query Layer that meet the requirements of both the spatial and geographic queries. All other points in the Query Layer will be displayed but will not be selected. For example, if we wanted to see all narcotics incidents within 1,000 feet of a school, the incident query layer would display all Incidents in the Query Layer and select only the narcotics within 1,000 feet of the school.



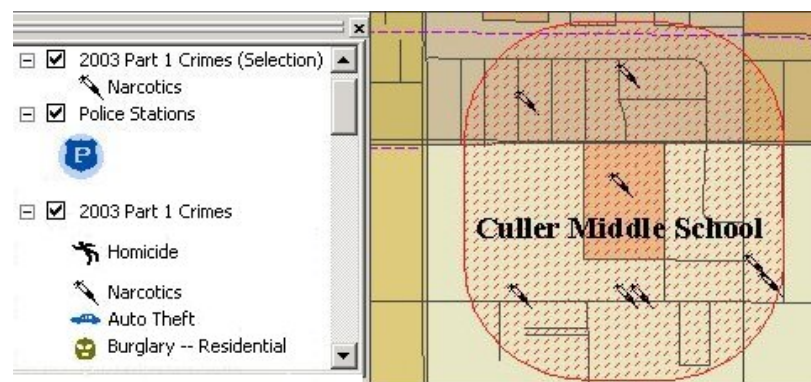
- **Show only saved query values and highlight selection**

This option will create a Definition Query on the Query Layer based on the attribute query and will select the incidents in the Query Layer that meet the requirements of the geographic queries. For example, if we wanted to see all narcotics incidents within 1,000 feet of a school, the incident query layer would display only the narcotics Incidents and select all the points within 1,000 ft of the school.

Attachment A

- **Show only selection (as new layer)**

This option will create a new selection layer from the Query Layer that meets the requirements of both the spatial and geographic queries. For example, if we wanted to see all narcotics incidents within 1,000 feet of a school, a new layer would be created that would display only the narcotics incidents within 1,000 ft of the school.

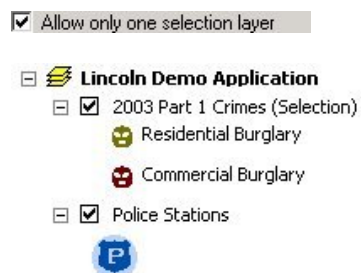


The new selection layer takes the following properties from the Query Layer:

- Primary Display Field, the field is used with map tips and is used to represent the feature in the left side of ArcMap's Identify Results window when you use the Identify tool.
- The visible fields and the field alias for the layers attribute table.
- The label field.
- The text symbol used for the labeling.

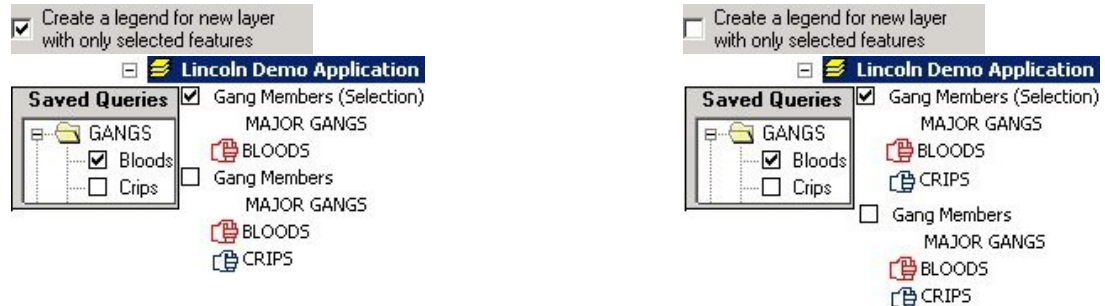
Allow only one selection layer

This setting enforces that there is only one [selection layer](#) per data frame. If an OmegaGIS routine is run and a new selection layer is output to a data frame with an existing selection layer, the existing layer is replaced with the new layer. This setting is only used when the query results are displayed as a new selection layer. This setting by default will only allow one selection layer.



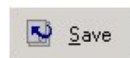
Attachment A**Create a legend for new layer with only selected features**

This setting, if checked, will create a subset of the existing query layer legend based on the result of the query routine. The resulting layer will only include legend items that are present in the underlying data of the new layer. If this setting is not checked, the entire legend will be displayed for the new layer. This setting is only used when the query results are displayed as a new selection layer. This setting by default creates a legend for new layers with only selected features.

**Other Query Results Settings**

- **Display the routine summary dialog**

This settings, when checked, displays the routine summary dialog after the completion of the data input for query, density, and analysis routines. The summary dialog provides an overview of the parameters for the last routine run. Use the Back button on the summary dialog to return to the query, density, or analysis routine dialogs to make any edits. The Save button, which is only present when running a query routine, allows the parameters to be saved as a [Cyclical Report](#) and/or [Threshold Alert](#). This setting by default displays the routine summary dialog.



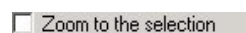
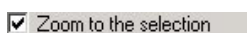
- **Shrink the OmegaGIS dialog when routine is complete**

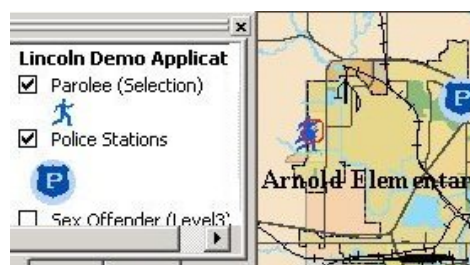
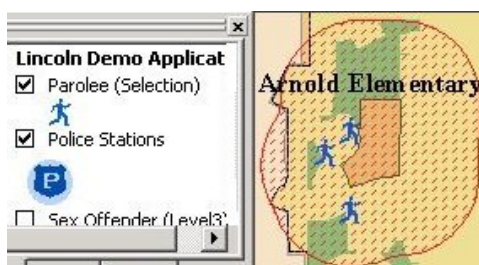
This setting will either shrink or hide the routine dialog when the routine has completed. When the dialog is shrunk, it can be expanded by double clicking the green Sherlock icon. Once expanded the routine parameters can be edited and the routine rerun, producing new results based on the edited information. When the dialog is hidden, it can only be accessed by reopening the Main Menu. The default for this setting is to shrink the dialog when the routine is complete.



- **Zoom to selection**

This setting, if enabled, zooms the data frame to the visible extent when the routine has completed. Different routines zoom to different extents based on the parameters specified in the routine. If a routine has a boundary layer or a user defined area specified, this setting will zoom the data frame to the extent of the geographic boundary. If the routine only contains an attribute query, then the data frame will be zoomed to the extent of either the selected incidents or the new selection layer. If this setting is not enabled, then the data frames extent will not be changed. By default the data frame is zoomed to the selection.

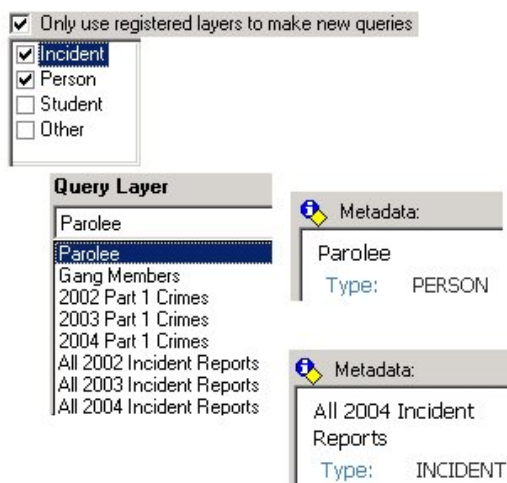


Attachment A**Registered Types**

This setting determines if only registered layers will be used as query layers in OmegaGIS routines. To register layers as 'Incident', 'Person', 'Student' or 'Other' use the OmegaGIS [Metadata Editor](#) in ArcCatalog.

- **Only use registered layers to make new queries**

This settings, if checked, will only populate the list of query layers with layers that have been registered. The list box below lists the registered types that can be used as query layers. Checking the box next to each registered type adds each layer of that type to the list of query layers in the OmegaGIS routines. Depending on these settings, the list of query layers will be limited to only those layers of interest for querying. If this setting is enabled, a registered type in the list box must be checked. By default this setting is disabled.

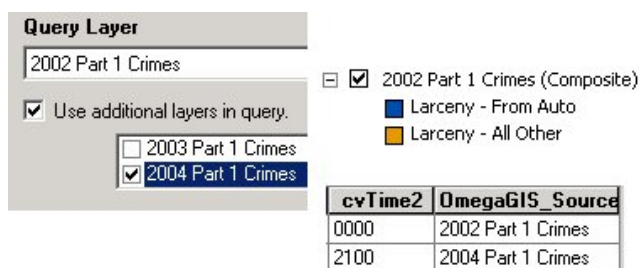
**Additional Query Layers**

These settings specify the options to be used when using [additional query layers](#).

When additional query layers are used, the incidents selected by the attribute query and/or spatial query, are exported as feature classes into a personal Geodatabase. The Geodatabase is named AddQueryLayers.MDB and is located in the "\Analyses" folder in the project workspace.

- **Create the 'OmegaGIS_Source' field that records the name of the source layer**

This setting when checked creates a new field in the new feature class named 'OmegaGIS_Source'. This new field will be populated with the name of the parent layer for each record. This allows for composite layers to be queried as to their source layer. The default for this setting adds the 'OmegaGIS_Source' field.

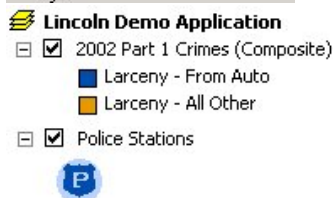


Attachment A

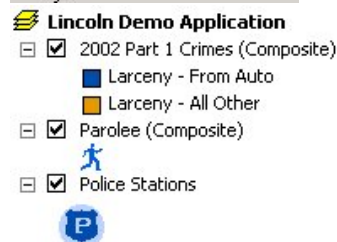
- **Only create one new composite layer from each master query layer**

This setting enforces that there is only one [composite layer](#) per data frame. If an OmegaGIS routine is run and a new composite layer is output to a data frame with an existing composite layer, the existing layer is replaced with the new layer. This setting by default will only allow one composite layer.

Only create one new composite layer from each master query layer



Only create one new composite layer from each master query layer



- **Additional Query Layer tool**

The additional query layer tool allows the user to compare two different layers from a specified data frame to see if they can be used as additional query layers in OmegaGIS routines. The tool opens a new dialog which requires the input of the data frame, the master query layer and the additional query layer. Once these parameters are inputted the results will be displayed in the output frame.

Data Frame

Lists all the data frames in the current map document. This will allow the user to specify the data frame of interest. The two layers being compared must be in the data frame selected.

Data Frame

Layers

The layers frame lists all the layers in the selected data frame. This will allow the user to specify the master and additional query layers of interest. Both the master and the additional query layers can be changed at any time for different comparison results.

Layers

Master Query Layer

Additional Query Layer

Output

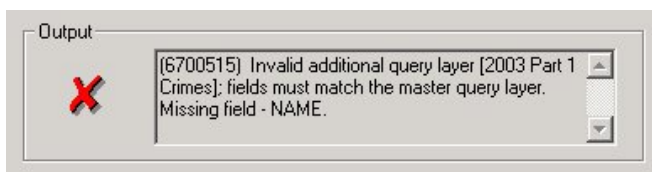
The output is displayed in the Output frame. This tool compares the layer criteria for the additional query layer as compared with the master layer. The layer criteria are described in the [additional query layer](#) topic of the help.

If a layer meets all the criteria of an additional query layer then a green check is displayed with the message 'Layer <master query layer> is an additional query layer of <additional query layer>.'

Output

Layer All 2004 Incident Reports is an additional query layer of layer All 2003 Incident Reports.

If a layer does not meet all the criteria of an additional query layer then a red X is displayed with the first layer criteria not met by the layer.

Attachment A**Advanced****OmegaGIS Layers**

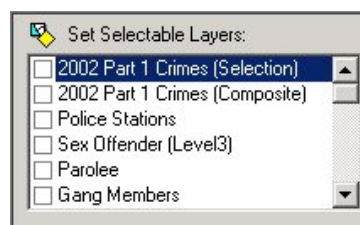
- **New layer added by OmegaGIS routine is selectable**

Toggles the ability for all layers created by OmegaGIS routines to be selectable in the data frame. Most layers in the data frame are not selectable. The default for this setting is to leave the new selection layer not selectable.

New layer added by OmegaGIS routine is selectable



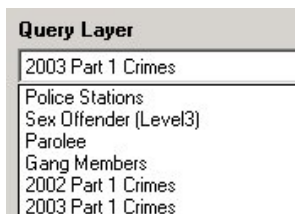
New layer added by OmegaGIS routine is selectable



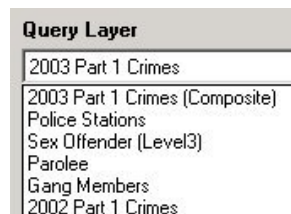
- **Exclude Composite layers created from OmegaGIS routines from being used in new queries**

This setting, when checked, will prevent composite layers from being used as [query layers](#) in OmegaGIS routines. Selection layers can never be used as a query layer regardless of this setting. This setting by default excludes Omega created layers from being used as query layers.

Exclude layers created from OmegaGIS routines from being used in new queries



Exclude layers created from OmegaGIS routines from being used in new queries

**Other Layers**

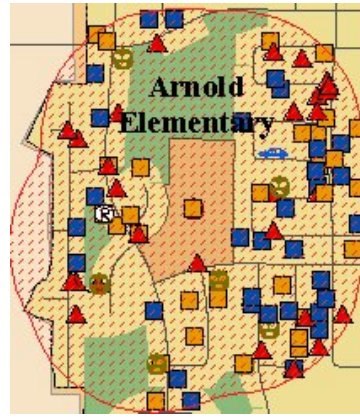
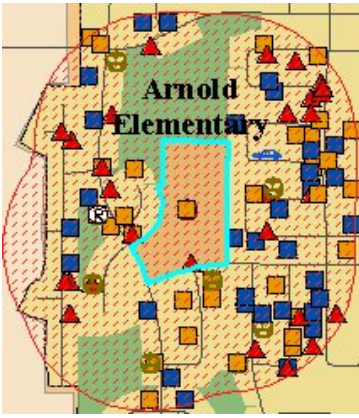
- **Select features used as boundaries, such as 'Police Beats', that are used with OmegaGIS routines**

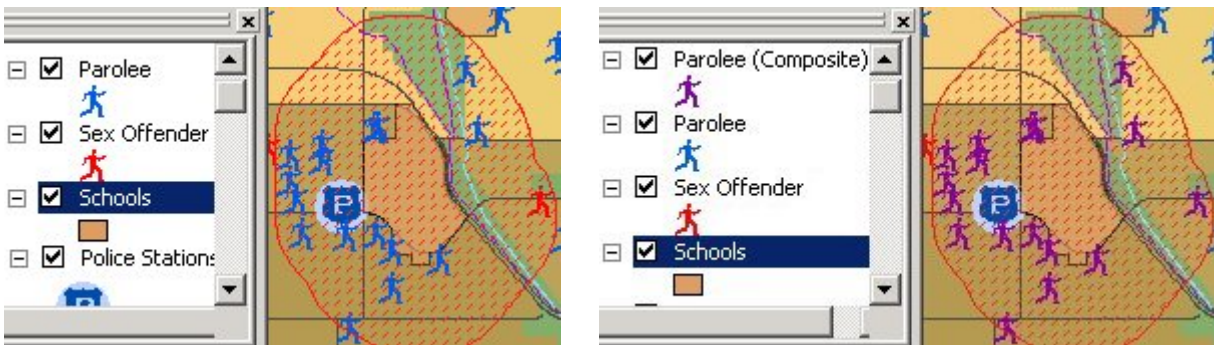
When geographic queries are performed, this setting, if checked, will select the boundary layers which meet the queries criteria. By default boundary layers are selected.

Select features used as boundaries, such as 'Police Beats', that are used with OmegaGIS routines

Select features used as boundaries, such as 'Police Beats', that are used with OmegaGIS routines

Attachment A



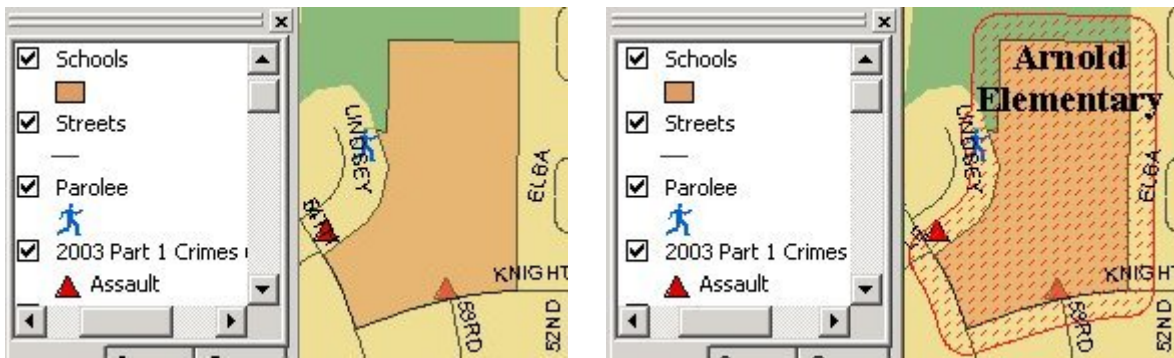
Attachment A

- **Remove OmegaGIS graphics, labels, and buffers.**

This setting deletes all graphics generated by OmegaGIS routines. This is accomplished by deleting all OmegaGIS [annotation groups](#) in the active data frame. Labels stored on the <Default> annotation group (typically street labels) will not be removed. The default for this setting is to clear all OmegaGIS graphics.

Remove OmegaGIS graphics, labels, and buffers.

Remove OmegaGIS graphics, labels, and buffers.

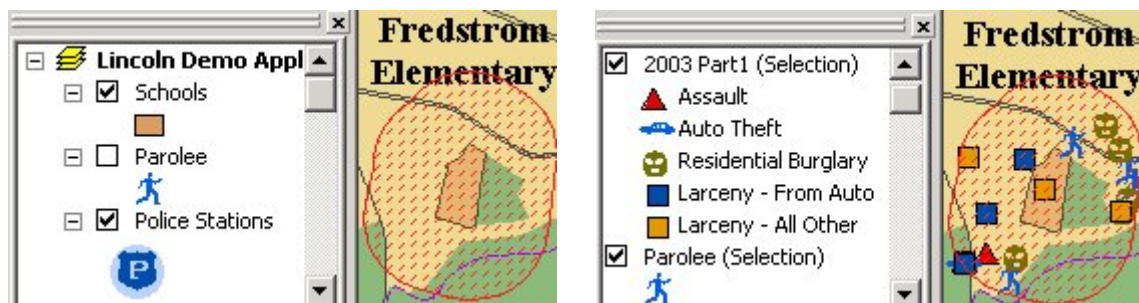


- **Remove selection layers.**

This setting will delete all of the [selection layers](#) from the active data frame. As a default, the selection layers will not be removed.

Remove all selection layers.

Remove all selection layers.

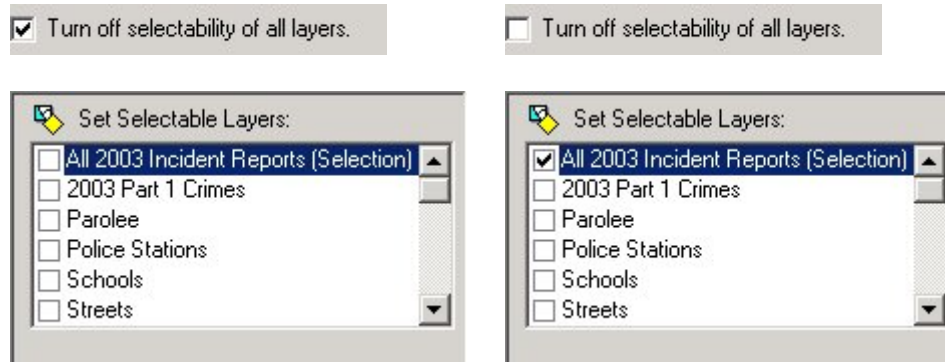


- **Turn off selectability of all layers**

This setting will cause the layers in the active data frame to not be selectable. Selectable layers can be set or unset on the [Omega tab](#) or on the Selection tab on the Table of contents.

Attachment A

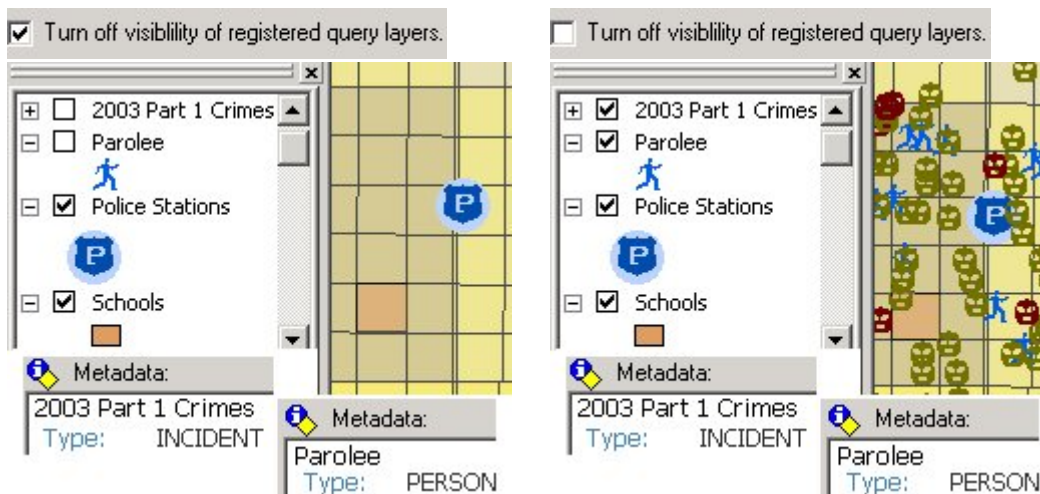
This setting's default is to turn off the selectability of all layers.



- **Turn off visibility of registered query layers.**

This setting will cause the registered [query layers](#) to not be drawn in the active data frame.

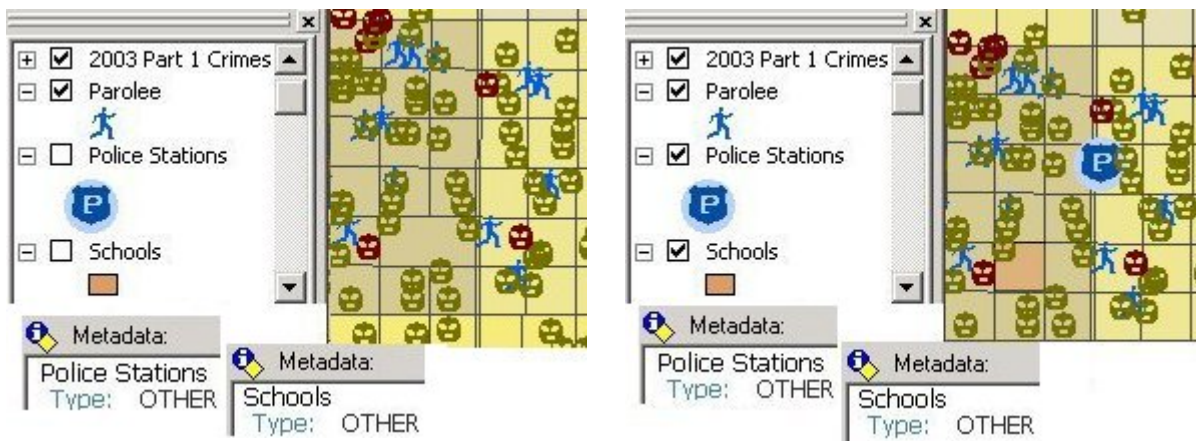
This setting only affects point layers. The default for this setting turns off the visibility of registered query layers.



- **Turn off visibility of layers that are registered as 'Other'.**

This setting will cause the registered [query layers](#) that are classified as 'Other' to not be drawn in the active data frame. As a default, layers registered as 'Other' will not be turned off.

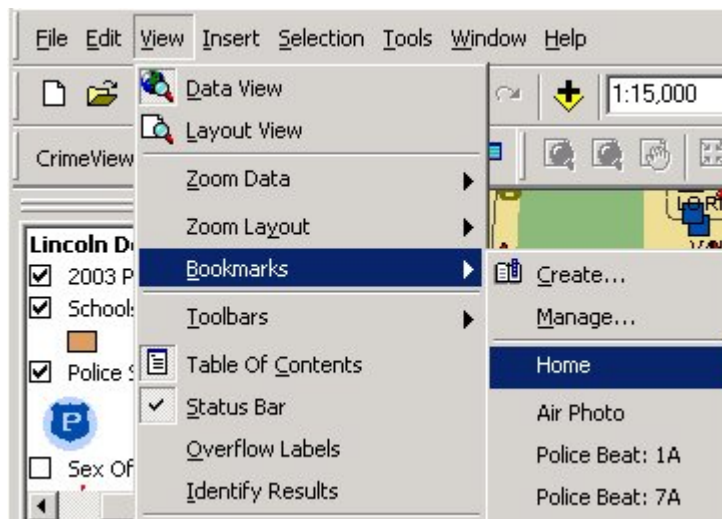


Attachment A

- **Zoom to:**

This setting when unchecked will not change of extent for the active data frame. If the setting is checked, the user has the choice of two options: Full Extent or Home. The Full Extent option will zoom to the full extent of all layers in the active data frame. The Home option will zoom to a preset bookmark named Home in the active data frame. If the bookmark is not found, the data frame will zoom to the full extent.

To create a bookmark, zoom the map to the area you want for Home; click the View > Bookmarks > Create item and name the bookmark "Home". The default for this setting zooms the data frame to Home.

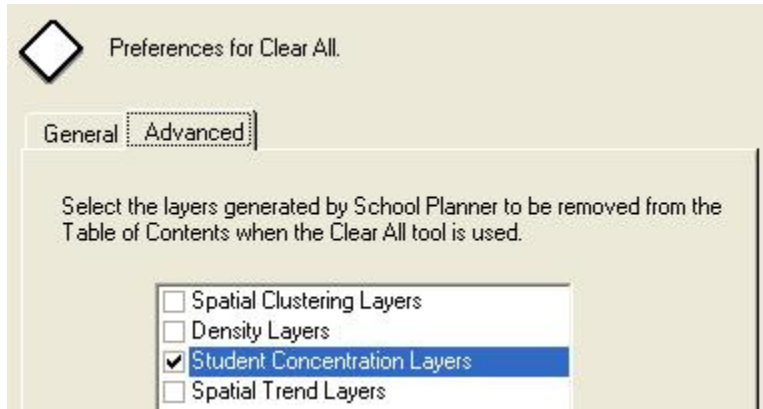


Advanced Tab

The Advanced Tab contains a list of all of the different types of layers generated by Omega routines. When a new layer is created, metadata is attached to the data source of the layer to identify the routine that generated it. If a layer type is selected from the Clear All list, when the Clear All is activated, those layers found in the ArcMap table of contents with the selected routine type are removed from table of contents and map.

During a Clear All, layers are removed from the table of contents and map if they have the appropriate routine type, but the data source of the layer remains on disk. When the project is closed however, if these layers no longer exist in the table of contents, the data source is deleted.

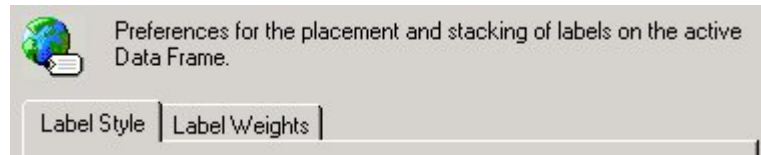
Attachment A



Setup: Labels

OmegaGIS routines use annotation groups to organize map document graphics. Annotation groups control the draw order (weights) of text, which allow buffers and labels to be drawn on top of existing graphics without blocking them. Also, annotation groups can associate with a layer which turns off the visibility of the label when the layer is turned off. Label symbol properties can also be set to display OmegaGIS routine labels in the same format as the label properties of the layer that is being labeled. All of these settings can be applied using two subcategories:

[Label Style](#)
[Label Weights](#)



Label Style

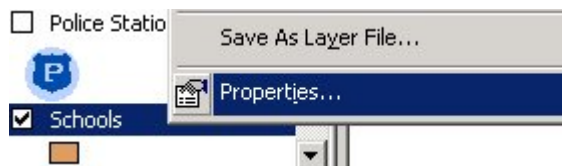
This subcategory sets the font, color, position, and look of the labels generated from running OmegaGIS routines.

Label Style:

This setting allows the user to choose the look of the labels generated from all routines other than the 'Near an Address' routine. The three options that can be set are as follows:

- **Use layer label properties**

The label font, color, size, position... are gathered from each layer in the labels tab on the layer properties dialog. The 'Layer Properties' dialog is accessed by right clicking on a layer in the table of contents and selecting the 'properties' item from the popup menu.

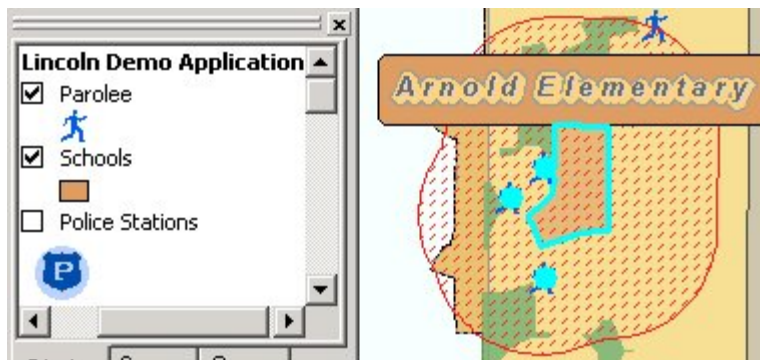


On the 'Label' tab, the 'Text Symbol' frame displays the current symbol used to label the text. Click the 'Symbol...' button to change these settings in the Symbol Selector dialog.

There are many options used to customize your text in the Symbol Selector dialog. Please refer to the ArcGIS Desktop help to further explore all the settings available in creating a customized text symbol.

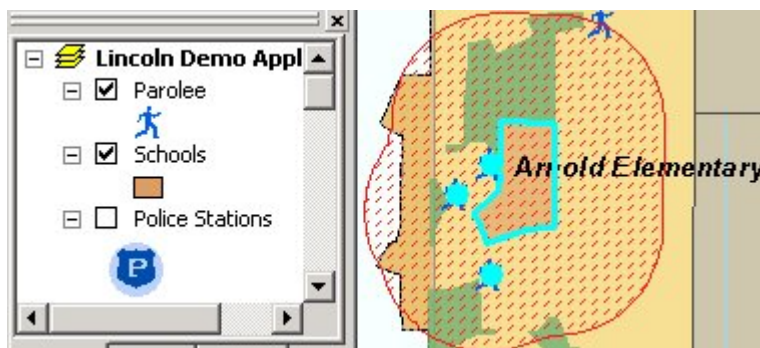


The 'Use layer label properties' setting is used as the default, since it gives the most flexibility in setting the look of the labels.

Attachment A

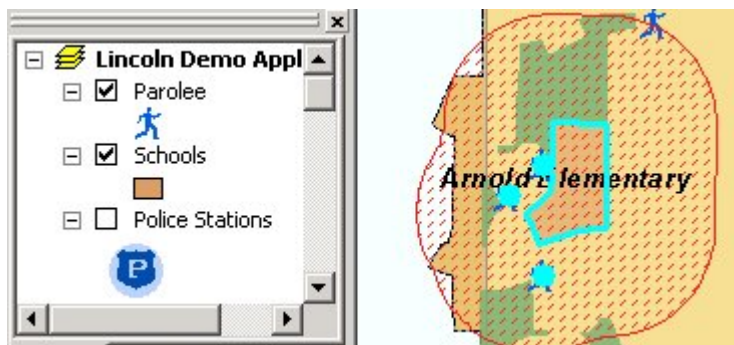
- **Left Justified**

This option displays left justified standard OmegaGIS font, which is black, Arial, 10 point, Italic, and Bold.



- **Center Justified**

This option displays center justified standard OmegaGIS font, which is black, Arial, 10 point, Italic, and Bold.



Near an Address label style:

This setting allows the user to choose the look of the labels generated from the ['Near an Address' routine](#). Each setting option will generate a label that contains the address text entered by the user in the **Where?** tab of the 'Near an Address' routine. All the labels generated from this routine will be included on the OmegaGIS Buffers annotation group. The three options that can be set are as follows:

- **Buffer Balloon Callout**

The text box that is generated from this setting is positioned just outside the upper right portion of the buffer and a leader line connects the box to the address. The address is

Attachment A

marked by a red 'X'. This is the default option.

- **Point Balloon Callout**

The text box that is generated from this setting is positioned at the upper right portion the address and has no leader line. The address is marked by a red 'X' that covered by the text box.

- **Text Only**

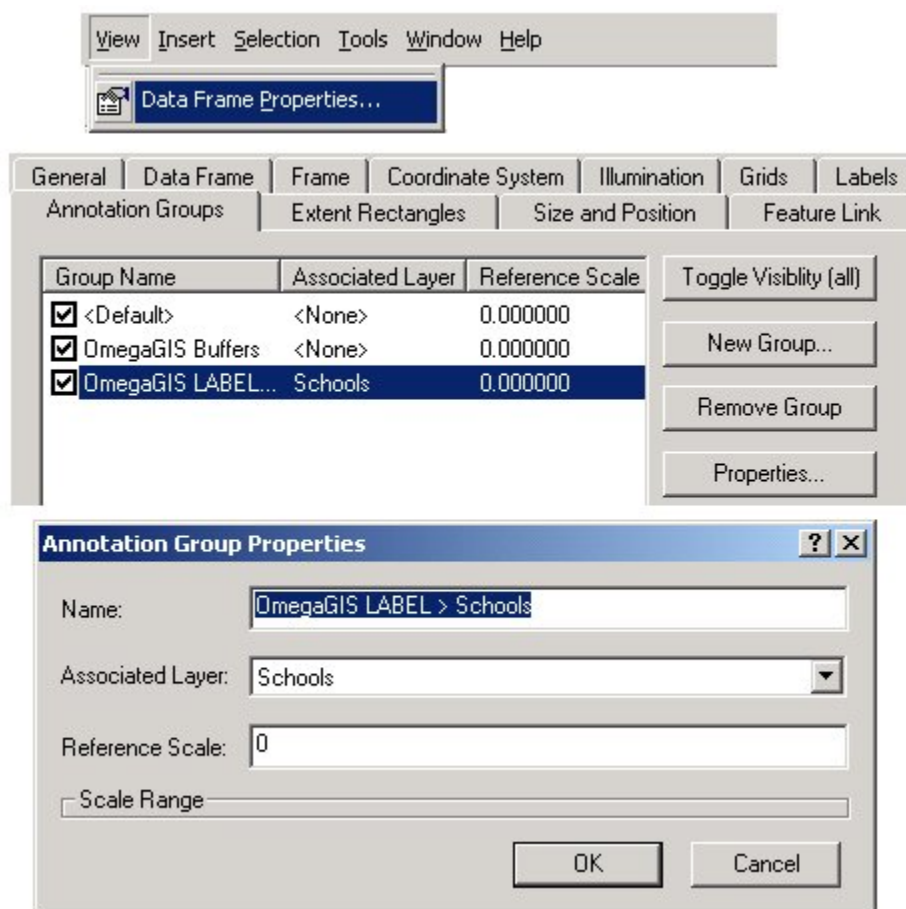
Text that is generated from this setting is positioned just outside the upper right portion the address and has no leader line. The address is marked by a red 'X'.

Label Weights

Annotation groups are stored in the map document and enable you to manage and organize graphics in the data frame.

Managing Annotation groups:

To manage the annotation groups in the active data frame, choose 'Data Frame Properties' from the 'View' menu and click the 'Annotation' tab. In this tab you can set a reference scale, assign an associated layer, toggle visibility, add new groups, and remove groups. To set a reference scale or associate the annotation group to a layer select an annotation layer and click the 'Properties' button.



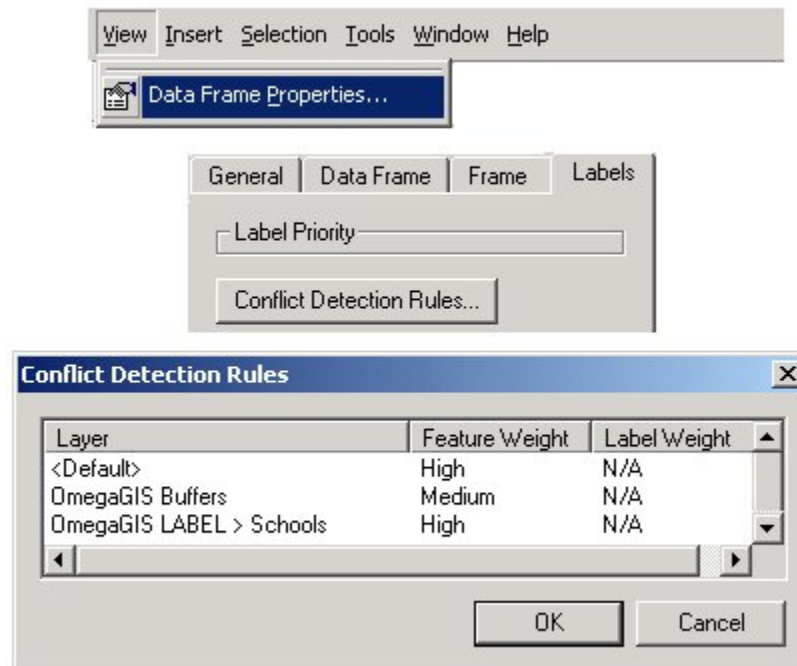
A reference scale of 0 will draw text at the same size regardless of your data frame's scale. If a reference scale is specified then the labels will draw at the specified size only when zoomed to that scale. If another scale is applied then the text will either get smaller or larger.

Attachment A

Associating a layer to an annotation group will make the labels in the annotation group turn off when the layer is turned off.

Organizing Annotation groups:

Graphic elements in the data frame can be drawn on different annotation group layers. Like layers in the table of contents, annotation groups have a draw order. In the table of contents, the draw order of layers is established from bottom to top, meaning that the bottom layer is drawn first and the top layer drawn on top of all other layers. Annotation group layers can be placed in a draw order by setting up conflict detection rules in the data frame. The conflict detection rules can be manually accessed by choosing 'Data Frame Properties' from the 'View' menu and click the 'Labels' tab.



These rules specify which annotation group has the lowest drawing priority and which has the highest. Annotation groups can have a weight of low, medium, or high. The general rule is that a graphic or label with a higher weight cannot be overlapped by a label with a lower weight. It follows that the user should give more important labels higher label weights. Within annotation groups draw order is established by the order by which the graphics are added. The first graphic is on bottom and the last graphic added is on top. The settings in this subcategory deal with assigning weights, or priority, to OmegaGIS annotation groups and to the default annotation group.

If you wish to know more about annotation groups and label placement, please refer to ArcGIS Desktop Help.

Note:

The settings for label weights will only take effect after an OmegaGIS routine is run.

- **Add labels to a new feature linked annotation group**

This setting creates a new or replaces an existing annotation group for the layer to be labeled in OmegaGIS routines with the exception of the 'Near an Address' routine. The new annotation group will only get created if the label check box on the **Where?** tab is checked.

It will be associated to the boundary or feature layer that it is labeling. The name of the new annotation group is always "OmegaGIS LABEL >" followed by the name of its associated

Attachment A

layer. Because this setting replaces an existing annotation group, if a routine is run where a previously labeled layer is labeled again, the previous annotation group and all of its graphics will be removed and recreated with the labels from the new routine. The default for this setting is to create a new annotation group for each OmegaGIS routine that creates labels.

- **Weight of new annotation group:**

This setting is used to specify the weight or drawing order of the new annotation group. This setting by default is set to High.

Tip:

In general, this setting should always be set to the same level as the default annotation group.

- **Weight of default annotation group:**

This setting is used to specify the weight or drawing order of the default annotation group. By default this setting is set to High.

The default annotation group contains the text added by dynamically labeling features. Only features labeled in this way will respond to this setup setting. Therefore, all text and other graphics manually added to the default annotation group will be displayed either on top or on bottom regardless of this setting. Dynamically labeled features are labels generated by the user right clicking on the layer to be labeled and selecting the menu item 'Label Features'.

Tip:

In general the default annotation group should be set to a weight above that of the buffer annotation group, so that buffers don't overpost geographic labels such as street names.

- **Weight of OmegaGIS buffer annotation group:**

This setting is used to specify the weight or drawing order of the OmegaGIS buffers annotation group. By default this setting is set to Medium.

The OmegaGIS Buffers annotation group is automatically created when either a routine is run that creates a buffer or a label is created for the 'Near an Address' routine. This annotation group is only created if it does not previously exist. If the OmegaGIS Buffers annotation group did previously exist and a routine is run where new graphics are created, these graphics will be added to the existing graphics in the annotation group. The name of the new annotation group is always "OmegaGIS Buffers", and this annotation group has no association to any layer.

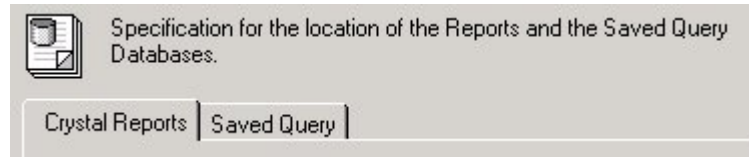
Tip:

In general the OmegaGIS Buffers annotation layer should be set to at least one weight less than the default annotation group. This is so geographic labels, such as street names, show through the buffer.

Setup: Databases (Locations)

Setup stores path information to the saved queries database and Crystal Report locations. This category stores and manages that path data. The subcategories reflect the types of paths stored:

[Crystal Reports](#)
[Saved Query](#)
[Street Network](#)



Crystal Reports

The Crystal Reports tab sets up the locations of the reports. These directories will be searched for Crystal Reports. One or more report locations can be defined. The order of the report locations is important. The Create Reports routine will search in the first directory, then the second, etc. The arrow keys can be used to change the priority of the report locations. The default report location is the reports folder in the project workspace.

- **Add**

Opens a browser dialog where the user can search the available local and network directories to select a file folder where Crystal Reports reside. The 'OK' button on this dialog will only be available when a folder is selected.

- **Remove**

This option deletes the selected Crystal Report location. This button will only be enabled when an location is selected.

To register specific reports to data layers use the [Metadata Editor](#) in ArcCatalog.

Saved Query

The Saved Queries tab is used to set up the locations of the saved query databases (Omega_Query.mdb). This is similar to setting the report locations on the previous tab. One or more saved query locations can be defined; the directories will be searched for existing saved query database. The order of the saved query locations is important. The saved query tree will search in the first saved query database, then the second, etc. The arrow keys can be used to change the priority of the saved query locations. The default location for the saved queries database is in the project directory.

- **Add**

Opens a browser dialog where the user can search the available local and network directories to select a file named Omega_Query.mdb. The 'OK' button on this dialog will only be available when this file is selected. This file contains the values used to populate the saved query tree used in OmegaGIS routines. To edit the saved query database use the [Saved Query Editor](#) in ArcCatalog.

- **Remove**

This option deletes the selected Saved Query database location. This button will only be enabled when an location is selected.

To register specific query groups to data layers use the [Metadata Editor](#) in ArcCatalog.

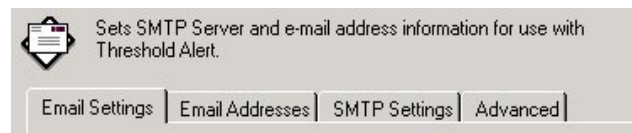
Attachment A**Street Network**

The Street Network location tab is available for FireView Setup only. Street Networks are created using the Omega Street Network tools on the Omega Data Manager toolbar in ArcCatalog. The default location that is searched for street networks is within the project directory structure under \Networks. Any additional locations that should be searched, must be entered using the **Add** button. The **Remove** button will delete the location, so that any routines using street networks will no longer search this folder.

Setup: Threshold Alert

[Threshold Alerts](#) require information on who will be alerted, how they will be alerted and with what information they be alerted. All these parameters must be set in order for Threshold Alerts to run. Each of the first three subcategories deals with one of these three aspects. The subcategories are:

[Email Settings](#)
[Email Addresses](#)
[SMTP Settings](#)
[Advanced](#)



The Email Settings subcategory allows the user to set the header information for the email. Email Addresses sets the recipients names and email addresses. SMTP Settings deal with the location of the email server on the network. And finally, the Advanced tab relates to optimizing the threshold alerts database.

NOTE:

SMTP Settings and Email Addresses are related, in that every email address must be associated with a server. For this reason it is HIGHLY recommended that the SMTP Settings be set BEFORE any Email Addresses are entered.

Email Settings

Email Settings lets the user specify custom header and subject information that will be included in the Threshold Alert email.

From email address

- **From email address**

This setting includes a text box where the user specifies the email address that will shown in the from line of the email header. The address must be in the format x@x.x and be longer than 6 characters in length.

- **Send a copy to this email address (CC)**

This setting carbon copies (CC) the email address entered in the text box above.

Email Subject Information

- **Threshold group and alert name**

This option will populate the subject line with the name of the Threshold Alert that is being run. This is also the name of the threshold alert group.

Alerts	
	Name
	Auto Theft
	Police Beat 1 > 1 Month

- **Number that exceeded threshold**

This will also include the number of incidents that occurred in the line of the subject.

Attachment A

Subject: Auto Theft: 1 alert(s) exceed threshold

Alerts	
	Name
	Auto Theft
	Police Beat 1 > 1 Month

- **Custom subject**

This text box allows the user to enter a custom subject for Threshold Alert emails.

Subject: Custom Subject

Alerts	
	Name
	Auto Theft
	Police Beat 1 > 1 Month

Email Addresses

Emails may be sent to any valid email address, however the Email Server must be identified for each address. Email addresses that are entered before any servers are set will be associated with a generic 'default' server. If the setup dialog is closed and a default server is not specified a warning message will be issued, the dialog will not close and the SMTP Settings tab will be displayed. For instructions on how to set a default server see the [SMTP Settings](#) header.

- **New...**

Preferably after the SMTP server information is set recipient information can be added by clicking the 'New...' button that opens a new dialog. This dialog is used to gather information about the recipient and about the server specific to the new email.

Recipient information

Recipient information

Name:

Email address:

Do not send email to this address

- **Name**

The text entered into this box should be a descriptive name of the recipient.

- **Email Address**

The text entered into this box specifies the email address for the recipient. The address must be in the format x@x.x and be longer than 6 characters in length.


- **Do not send email to this address**

Checking this box will not allow email to be sent to the specified recipient. This setting could be helpful if the user wants to set up an email address and even include this email address in the alerts notification, but not have any mail sent to the addressee. Checking this box will give the email a grayed out icon.

Do not send email to this address

Name	Email Address
 The Chief	Chief@PoliceDepartment.com

Do not send email to this address

Name	Email Address
 The Chief	Chief@PoliceDepartment.com

SMTP server information (optional)

This setting is optional because by default all new emails are associated with the default SMTP server. This setting allows the user to set emails to different servers.

Attachment A**NOTE:**

If only one SMTP server is used then this setting can be ignored.

This setting includes a tag that tells the user the current default SMTP server. There are two different messages displayed in this tag to aid the user in selecting the appropriate server for the email. The tags are as follows:

The Default SMTP server is: <SERVER NAME>

This will be displayed if a default SMTP server is set. If there is only one SMTP server set and it is designated as the default the rest of the settings in this option will not be available. Otherwise if there are multiple servers another could be assigned to this email.

There is no default SMTP server.

This message will be shown either if there are no servers set or if there are no default server set. In either case if another server is not assigned each new email would be given a generic 'default' server which would be assigned to the emails when the actual default server is set in the SMTP settings tab.

- **Select an SMTP server for this email that is different than the default**

The default server is always used for a new email by default. This checkbox allows the user to override that setting and specify a server that is not the default if it has been added to the SMTP server list in the SMTP settings tab.

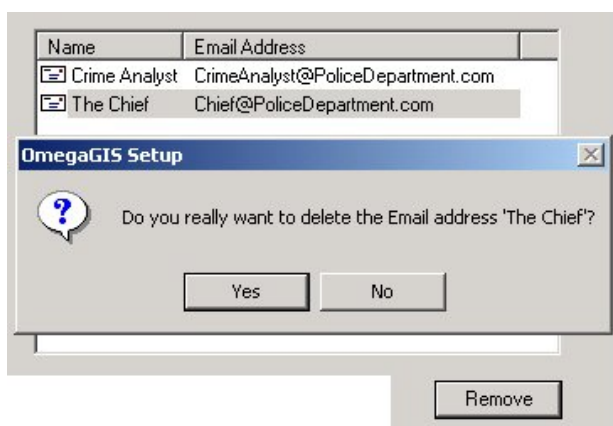
If this box is checked then the list below will be populated with all the SMTP servers in the SMTP server list that are not the default. Another server must be chosen if this box is checked.

- **Edit...**

Clicking this button, allows the user to edit all the information about a selected email address. The same dialog opens as when the 'New...' button is clicked, with the exception that it is populated with the information about the selected email. The recipients information or the SMTP server information can then be updated and saved.

- **Remove**

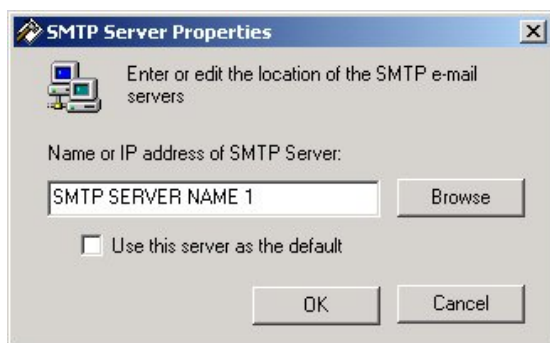
This option deletes the selected email address. This button will only be enabled when an email is selected.

Attachment A**SMTP Settings**

In order to send Threshold Alerts to the appropriate personnel, an SMTP server must be selected. The first step in setting up the SMTP Server information is to research the names or IP addresses of the SMTP server used at your site. Contact your system administrator for this information.

- **New...**

When the Names or IP addresses are acquired, they can be entered into a list using the New button. Clicking on the New button opens a dialog which provides a text box for either the Name or the IP address. This information can be entered manually or browsed from a list of servers on your network.

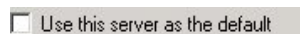
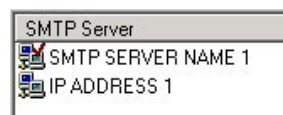
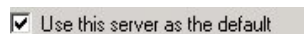


- **Name or IP address of SMTP server:**

The text entered into this box should contain the name of the IP address or the server name received from your system administrator. The server name can be manually typed in or the servers on your network can be accessed by clicking the browse button.

- **Use this server as the default**

Selecting this check box automatically assigns the server to any email address entered after the default server is set. The default server is identified by a red checkmark within the icon, next to its name in the list. This setting should always be used if there is only one server that will be added. If there are multiple servers being added then set the default server to the server which is associated to the most emails.



- **Edit...**

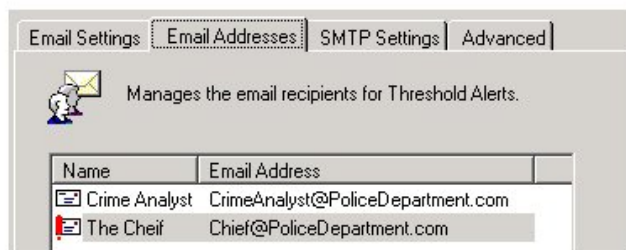
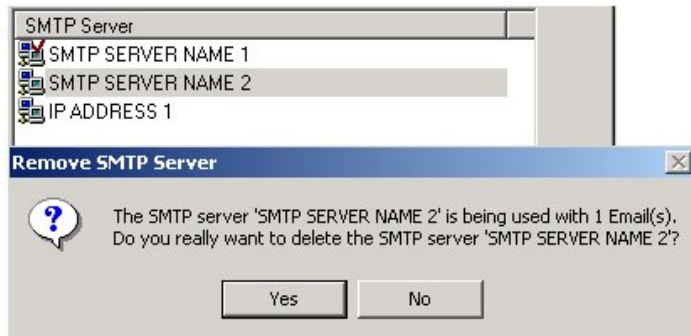
Clicking this button, allows the user to edit all the information about a selected SMTP server or IP address. The same dialog opens as when the 'New...' button is clicked, with the exception that it is populated with the information about the selected server. The server name and default status can then be updated and saved.

Attachment A

- **Remove**

This option deletes the selected SMTP server or IP address. This button will only be enabled when a server is selected. If a server that is attached to an email is attempted to be removed a message box will appear notifying the user. Emails associated with that server will have a letter icon with a red exclamation point.

If this occurs go into the Email Addresses tab and repoint all the addresses that have the new icon to a new server by clicking the 'Edit...!' button.



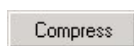
Advanced

The Advanced tab allows the user to use some simple database management tools to optimize the performance of the threshold alert database.

Database Tools

- **Compress**

Email address and server information is saved to the Threshold Alert personal geodatabase in the project folder. If many edits to the database are made, it is a good idea to compress the database as it can become large due to the accumulation of edits and deletions.



History Files

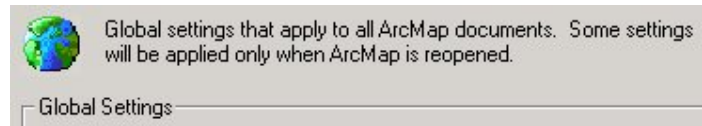
- **Clear History**

This setting is available to keep the size of the database manageable. History records refer to those records that track when a threshold is sent. They should be deleted from the database when this information is no longer required.



Setup: Global

Global settings apply to all ArcMap Documents. Changes to the Global settings will take affect the next time the ArcMap document is opened.

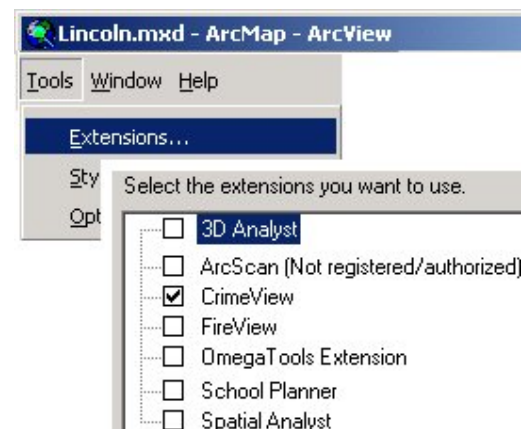
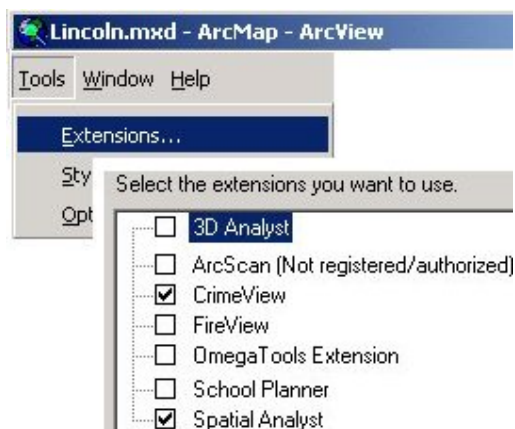
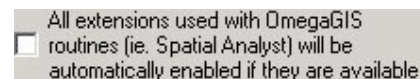
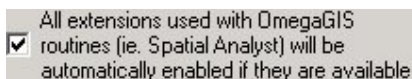


- **Splash Screen displayed on startup**

The Omega Desktop splash screen is displayed on the start of ArcMap. When this setting is checked the splash screen will be displayed.

- **All extensions used with OmegaGIS routines (ie. Spatial Analyst) will be automatically enabled if they are available**

The Spatial Analyst extension is used in the OmegaGIS Density routines and in the Analysis routine Spatial Trend. To use these routines, Spatial Analyst must be licensed and enabled on the current machine. For information about installing and licensing ESRI extensions please use ArcGIS Desktop Help. This setting automatically enables Spatial Analysis or any other necessary extension when the OmegaGIS extension is enabled.



- **Previous Week Date Range**

The date/time control has the functionality to select a date range for the previous week. The day of the week to use for the start of the week is controlled by this setting. The default date of the week is Sunday.

- **Crystal Reports**

The Crystal Reports version to be used when opening the reports is controlled by this setting. The user can choose from the selection of available versions. The default version used is Crystal Reports 11.5. For information about the number and names of Crystal Reports versions installed on the users machine click "Get Installed Versions".

Performance And Tuning

Enhancing the performance of ArcGIS and OmegaGIS software can be accomplished by using several of the tips and best practices that are outlined in the following sections. Designing a project that leverages all of the benefits of both ArcGIS and OmegaGIS requires some preparation during the initial stages of project design. It is important to spend some time reviewing the architecture, as well as the software settings in order to tune the project to run as fast and as efficiently as possible.

Performance Checklist

Hardware

- Computer meets Omega [hardware requirements](#).
- Follow [computer maintenance](#) practices.
- [Network](#) is good operating order.

GIS Data

- Large datasets that rarely change are on [local machine](#).
- Geographic data stored in [personal geodatabase](#) rather than a shapefile.
- Number of [fields](#) in incident data kept to a minimum.
- Limit the number of [records](#) in layer.
- All layers should share the same [projected coordinate system](#).
- [Rasters](#) should have pyramids built.

ArcMap Tuning

- Limit number of [layers](#) in ArcMap document.
- Use tools for [map navigation](#).
- Do not use [map tips](#).
- Use [scale dependency](#) for layers and labels.

ArcCatalog Tuning

- Use folder [shortcuts](#).
- Limit files [displayed](#).

OmegaGIS Setup Tuning

- Follow best practices for [OmegaGIS setup](#).

OmegaGIS Tuning

- Limit number of [saved queries](#).
- [Compress](#) personal geodatabases.
- Use [spatial and attribute](#) queries when using OmegaGIS routines.

Hardware

This topic outlines the best practices and recommendations for hardware when using ArcGIS and OmegaGIS.

[Hardware requirements](#)

[Computer Maintenance](#)

[Network](#)

Hardware Requirements

The Omega Group suggests that for Minimum Requirements, the following hardware suggestions be followed.

Processor: Intel Dual Core

Memory/RAM: 2 GB or greater

RAM and the Pagefile are used by Windows XP to store temporary data as operations are performed by the operating system. Windows XP tends to require significant amounts of RAM, and often exceeds the allotted RAM for the machine. When this overflow occurs, information is saved to the Pagefile.

Unfortunately, reading and writing to the Pagefile results in reading and writing to disk, and can bog down performance. If the Pagefile size is too small, it becomes fragmented across the disk, and can further slow down a machine.

It is therefore important to have enough RAM and a large enough Pagefile size to operate efficiently. Omega recommends at least 2 GB of RAM . The general rule for the Pagefile size is 2X the RAM. The Pagefile cannot exceed 4095 KB, as this is the limit set for Windows XP.

Free Disk Space: 10 GB NTFS

Disk space is critical to maintaining a stable system. When disk space becomes low, performance can degrade, and system crashes occur more frequently.

Video Card: 256 MB or greater

When dealing with complex graphic files it is important to have a good video card that enables applications to quickly draw and refresh images. If a video card can only cache a small amount of data, the result is slow performance.

Computer Maintenance

Disk Space

Disk space is critical to maintaining a stable system. When free disk space becomes low, performance can degrade, and system crashes occur more frequently. There are several places on a computer that can become bogged down with temporary files created by different applications. The Temp directory is a common location for applications to store temporary files. In some cases these files are removed automatically, however, often they are not. Empty the temp directory of files to increase disk space where possible. When files are removed from the Temp folder in Windows Explorer, the files may be moved to the Recycle Bin. To ensure space is cleared on disk, clear the Recycle Bin of files.

If using the Internet frequently, numerous files can accumulate that are created when visiting different web sites. Using Internet Explorer click on Tools > Internet Options and select the General Tab. Delete the temporary internet files using the buttons provided, and clear the history folder.

Disk Fragmentation

Attachment A

Disk fragmentation occurs when files are added to or removed from disk. As disk fragmentation worsens the reliability and stability of a system degrades. Four effects of a fragmented disk include, increased boot up time, increased shut down time, an increase in the number of system crashes and slower or no response times from applications and the operating system.

To avoid problems with fragmented disks, use the Disk Defragmenter tool available from Start > Programs > Accessories > System Tools.

Applications and Processes

Windows XP is configured to 'multitask' between applications so that it appears that these processes are occurring simultaneously. In fact, the operating system is actually switching rapidly between processes, executing one at a time. This rapid switching between applications or 'multitasking' is the reason that as more processes are added, the slower the operating system performs.

The first defense for removing the effects of multitasking is to identify any applications, processes, features or services that are unnecessary. In the lower right corner of the computer screen, a system tray identifies some of the applications running in the background. Remove the applications that are not required. To turn off services, right click on My Computer and select 'Manage'. Expand the 'Services and Applications' menu item to identify those unnecessary services. However, do not remove services if you are unsure.

Personalized Menus, a feature of Windows XP, tracks menu items opened frequently and hides those rarely used. This process requires significant memory and can slow down performance. To turn off this feature, access Start > Settings > Taskbar and Start Menu and uncheck the 'Use Personalized Menus'.

Other features requiring large memory overhead can be found by right clicking on the Desktop, and selecting Properties > Effects. Turn off 'Use Transition Effects...', 'Smooth edges of screen fonts', and 'Show window contents when dragging'. Finally, in Windows Explorer, select Tools > Folder Options > General and set the Web View to 'Use Windows Classic Folders'. Windows will no longer create thumbnails for each file, which is memory consuming when complex images are selected.

Network

Many agencies using ArcGIS require that data central to GIS analysis be housed on a central server so that current information can be shared effectively. Moving large GIS datasets across a network however, can result in significant degradation in performance. The following recommendations and suggestions are aimed at the practices of the IT department of an agency in order to optimize performance for users of GIS data and software. Omega recommends GigaBit Nic (Network Interface Cards) for good speed.

There is some evidence that in switching from Windows NT to Windows XP, there is a significant drop in performance over a network. Consequently, it is important to ensure that network cable problems are resolved, since any problems are exaggerated by the higher network traffic. To ensure cables are in optimum condition, check for shorted patch cables and bad switch connections.

GIS Data

ArcGIS consists of ArcMap and ArcCatalog. Both of these components can be fine tuned in order to deliver faster performance when browsing or viewing large GIS datasets. In accessing GIS files, it is important to understand the impact of the file location on the speed and response time of these applications. This section has the following topics:

[Local Data](#)
[Data Format](#)
[ArcSDE](#)
[Coordinate System](#)
[Raster Files](#)

Local Data

Generally, GIS departments prefer to locate GIS data to be shared by all users in a central location, such as on a server, where it can be updated easily, and data redundancy is kept to a minimum. If users are accessing this data across a network, ArcMap and ArcCatalog may appear exceedingly slow.

Copying large datasets locally increases performance significantly, and should be considered when creating a GIS system architecture. Omega recommends that file-based data that rarely changes, such as street centerlines or police beats, be copied to the local machine. Only data that is updated frequently, such as incident data that is updated by the Omega Import Wizard, should be on a centralized server.

Data Format

With the advent of the personal geodatabase (MDB), a further advance is available to decrease the time it takes to access files across a network, or locally. As ArcGIS is tuned to work with the personal geodatabases, faster speeds can be achieved when shapefiles are converted to personal geodatabases.

In recent tests, the retrieval times of the personal geodatabase exceeded those of the shapefile both locally and over a network.

There is no longer a ten character limit on field names in the personal geodatabase as is the case with the shapefile format. The field name limit becomes a problem when creating shapefiles from other sources. When the field names are cut off to suit the ten character limit, occasionally duplicate field names are created.

Finally, the personal geodatabase supports a larger file size. The speed in retrieving information from a personal geodatabase does not start to degrade until the file size reaches about 250 MB.

Omega recommends the use of the personal geodatabase over shapefiles when possible.

ArcSDE

When working with large geographic datasets, ArcSDE provides an excellent alternative to storing geographic data in file based systems. ArcSDE is a gateway that enables the management of geographic data in database management systems. The software manages the access and distribution of spatial data to multiple users.

There are a number of ways to tune ArcSDE that can be used to increase performance depending on the architecture of the GIS system. The Omega Group can provide information as to whether ArcSDE is a viable investment as there are costs associated with the additional hardware and

Attachment A

software required to use this approach.

Limit Fields

To keep the incident data file small, the number of fields should be limited to those required to do analysis with OmegaGIS. OmegaGIS routines frequently cycle through field lists within layers. By keeping the number of fields down, the number of times a routine must loop through the list of fields is kept to a minimum. Additionally, limiting the number of fields will reduce the overall size on disk of the GIS file.

Limit Number of Records

Apart from limiting the number of fields within the incident data file, the number of records can be reduced by splitting up the GIS file either geographically or historically. Since OmegaGIS routines can accommodate querying multiple layers, sub-setting the data is now possible.

Omega recommends that a shapefile contain not more than 100,000 records and a personal geodatabase not contain more than 250,000 records.

Spatial Index

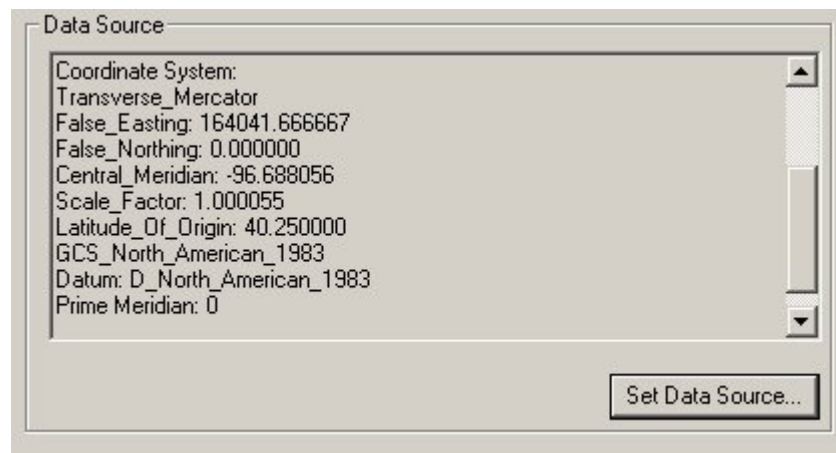
Indexes always increase the speed with which features can be searched within geographic files. Ensure that spatial indexes have been created on all layers that are frequently used in geographic analysis. A quick way of determining whether a spatial index exists is to right click on the layer name in the table of contents, open 'Properties' and select the 'Display' tab. If a spatial index does not exist for the layer, the 'Map Tips' option will be disabled. Spatial indexes are automatically created for personal geodatabase layers, while, shapefiles must have the index explicitly set.

Coordinate Systems

Coordinate systems provide the capability to locate points on the Earth's surface. A coordinate system may be either geographic or projected. A geographic system locates positions on the earth's spheroid, while a projected coordinate system undergoes a 'map projection' to locate points on a flat surface.

Omega recommends that a projected coordinate system should always be used when performing spatial analysis in ArcMap. This is because geographic coordinate systems do not deliver accurate measurements. Aside from creating a more accurate environment for spatial analysis, ensuring each layer within an ArcMap project is projected into the same coordinate system also increases performance. Since the layers share the same projection, they do not need to be re-projected on the fly, and this results in increased performance.

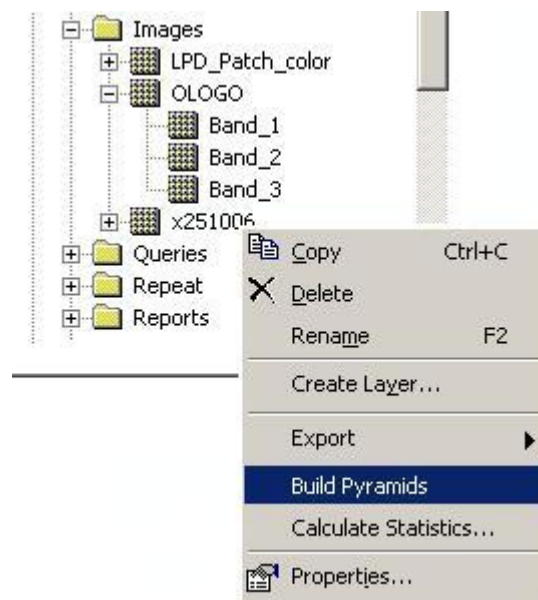
To determine a layer's spatial reference in ArcMap, right click on the layer name and select Properties. Click the Source Tab, the Coordinate System is shown in the Data Source Textbox.

Attachment A**Raster Files**

Raster files are images that are divided up by cells in order to create a smooth picture of a geographic area. Raster files typically take up significant amounts of disk space, and are slow to draw. Constructing pyramids for raster files is an excellent way to reduce on the amount of time it takes to refresh raster data on the screen.

Pyramids are multiscaled, resampled versions of the raster data. Without a pyramid the entire dataset is read from disk and resampled to a smaller size. Pyramids reduce the amount of time reading from the disk, by displaying less data as the user zooms out of the raster.

A pyramid can be created very easily by right clicking on the raster name in ArcCatalog and selecting the Build Pyramid option. To enhance performance further, switch the Display Quality option from Normal to Medium. This option is available in ArcMap, by right clicking on the layer name in the table of contents, selecting Properties and the Display tab.



ArcMap Tuning

This section outlines Omega recommendations to improve the performance of ArcMap.

[Data Inclusion](#)

[Map Navigation](#)

[Map Features](#)

Data Inclusion

When designing a new ArcMap project, it is important to keep in mind the impact of the data included in the project on performance. The number of layers added to a project, should be limited to those used in analysis. If additional layers are required for visualization purposes, they can be turned off while running routines.

It is also possible to set the layers to be automatically invisible when they are added to the project by selecting the Tools menu > Options and the Application Tab.

Map Navigation

Bookmarks

Bookmarks provide an excellent way to create points of interest on a map that can be revisited easily. Navigating by use of a bookmark is often faster than using the pan and zoom tools available from the ArcMap toolbar.

To create a bookmark, zoom to the area of interest, and select View > Bookmarks > Create from the ArcMap menu. Enter the name of the bookmark. Zooming to the area is now easily replicated by clicking on the name of the bookmark.

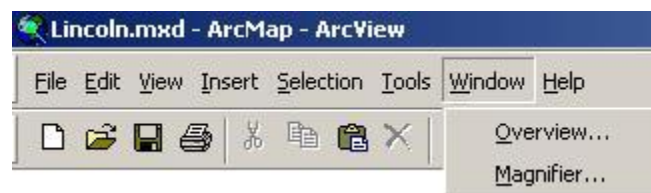
Layer Overview Tool

To access the Overview tool, click on Window > Overview and an overview window appears on the screen, from which you can view the full extent of the data in the project. The red highlighted box represents the layer on which the overview tool is based.

The Overview tool can be used to easily pan throughout the extent of the active data frame while limiting the number of times the data frame must be refreshed.

Magnification Tool

The Magnification tool is useful to view details on the map without having to use the pan or zoom tools. The Identify and Select Features tools can be used within the magnification window. To access the tool, click on Window > Magnifier. A magnification window will appear on the map.



Right click on the title bar of the window and ensure that 'Update While Dragging' is not selected. This feature updates the window frame by frame as it is moved across the map, and slows down the performance of the tool.

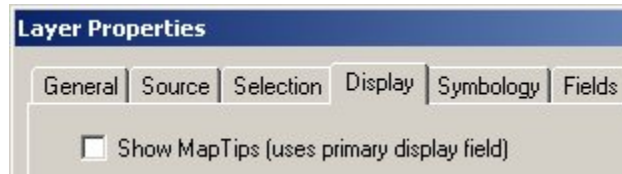
Map Features

Map Tips

Attachment A

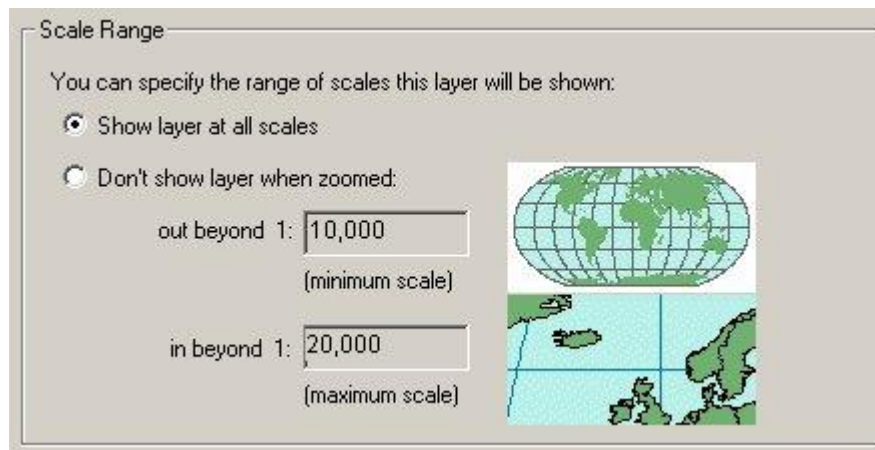
Map Tips show information about features in a layer based on their display field. By hovering over the feature on the map, a popup window opens to show the field value without the use of the interactive tool. Although this feature can be extremely helpful for users investigating the map, the tool does interfere with the Zoom In and Zoom Out capabilities of ArcMap, and may slow these processes down. To limit the impact of Map Tips, only turn the map tips on for those layers that are necessary.

To remove Map Tips from a layer, right click on the layer name in the table of contents, and select 'Properties'. Click on the display tab, and toggle the 'Show Map Tips' setting.



Scale Dependency

Scale dependency refers to the scale at which a layer is displayed within the project. For layers with a high level of detail, at smaller scales it is a good idea to make them invisible as refreshing them on the screen can take considerable time and resources. To set the scale dependency of a layer, right click on the layer name in the table of contents and select Properties. Select the General Tab, and enter the appropriate maximum and minimum scale range at which to display the layer.



Graphics and Symbology

The greater the complexity of symbols, the slower they are to draw on the map. Keeping symbology and graphics simple improves performance. Halos on large amounts of text are especially slow to display. Text shadowing can be used in place of halos, and at a lower cost to performance. Simplicity of symbology to improve performance, also applies to lines. Dashed and patterned lines display more slowly. Limit the use of complex lines where possible.

The advanced drawing options available by right clicking on the data frame, control how the symbols on the map are drawn. This feature does slow performance due to the fact that multiple redraws must take place to display the symbols. Avoid the Advanced Draw Symbol options unless necessary.

Label Scale Range

When displaying labels on the map, a scale dependency can be set explicitly for the labels. Right

Attachment A

click on the layer name, select Properties, and the Labels Tab. A scale range can then be set to view labels only at an appropriate scale.

ArcCatalog Tuning

ArcCatalog provides the interface for viewing and browsing GIS data. Depending on the size and complexity of the files, previewing and connecting to the data may occur more slowly. Outlined are Omega's recommendation for improving performance.

[Folder Shortcut](#)

[Limit Files Displayed](#)

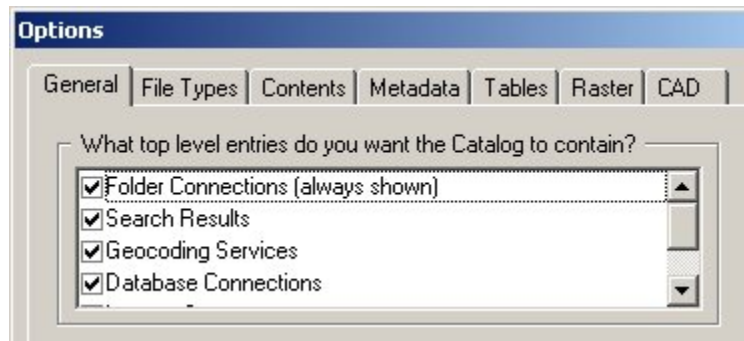
Folder Shortcut

To reduce the amount of time browsing for files, create shortcuts to folders and databases containing GIS information. From the File pull-down menu in ArcCatalog, select Connect Folder and then dialog that opens, browse to the folder to create the shortcut for.

Limit Files Displayed

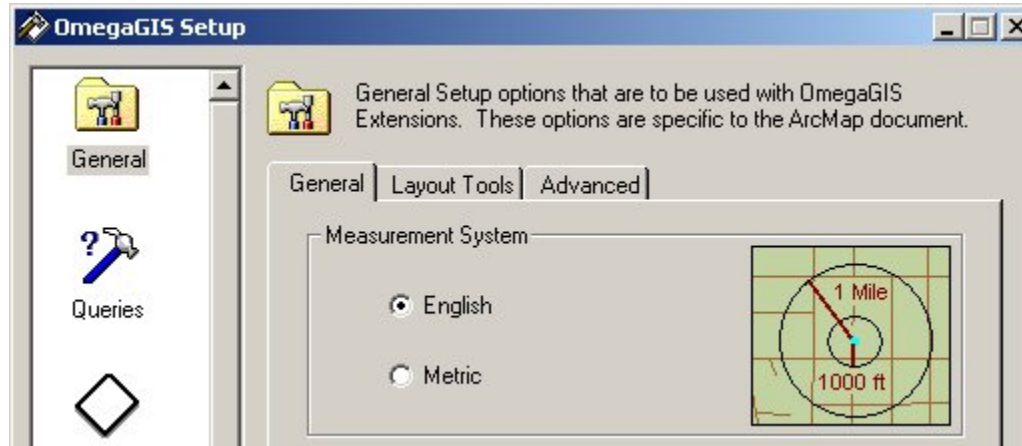
The types of files displayed by ArcCatalog can be narrowed by using the Tools > Options dialog to determine which top level entries and data types to display. A top level entry might be a folder or database connection, while a data type might include a shapefile or personal geodatabase.

An option exists in the same location to display only those files that contain GIS data. Enabling this option however slows down the rate at which files are displayed as they are searched each time for GIS data. Disable this option to ensure faster performance.



Omega Setup Tuning

[Omega Setup](#) is a feature of Omega Desktop software in which predefined settings can be maintained during the use of the routines in the project. Many of these settings and options are designed to improve performance while conducting analysis on large and complex geographic datasets.

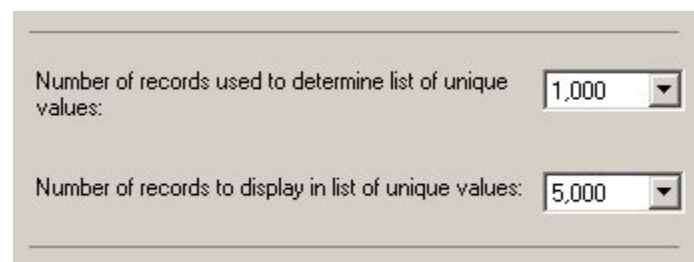


The following items from Omega Setup are identified as performance saving features, and should be set appropriately when initiating a new Omega Desktop project.

- [Unique Field Values](#)
- [Selection Layers](#)
- [Summary Dialog](#)
- [Registered Type](#)
- [OmegaGIS Layers](#)
- [Composite Layers](#)
- [Map Thumbnail](#)
- [Splash Screen](#)

Unique Field Values

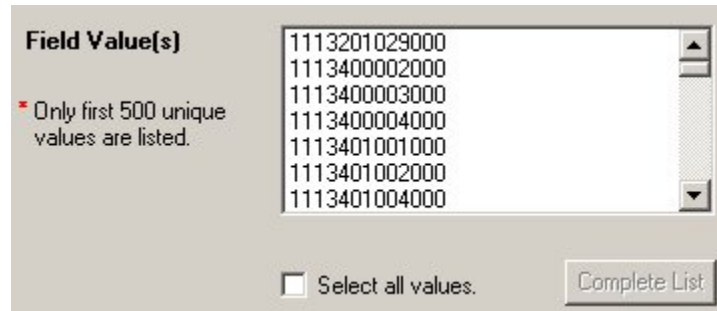
In most OmegaGIS routines, the 'Select By Field Value' option exists to select polygons from a map layer using the values from the attribute table associated with the selected layer. For very large datasets, with thousands of records, updating the field list on the dialog can be slow. There are two settings available that can speed the time it takes to update the field value list. Both settings are available on the Advanced Tab of the General Settings category.



The 'Number of records used to determine unique list of values' option, displays a range of values from 300 to 10,000. Selecting one of these values determines the number of polygons in the layer that will be sampled for unique values in order to populate the field values list box on the routine dialog. For instance, for a parcel layer consisting of 50,000 polygons, if the value is set to 10,000, only 10,000 polygons within the parcel layer will be sampled for unique values.

Attachment A

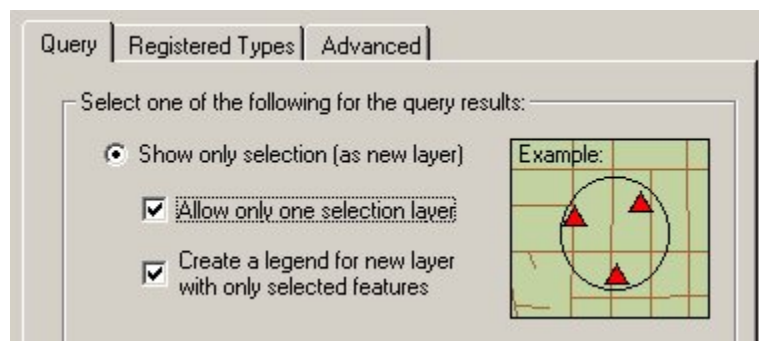
The 'Number of records to display in unique values list' option describes the actual number of records that will populate the list of field values. For instance, if 10,000 records are sampled from the parcel layer, and this option is set to 5,000. Only 5,000 field values will be listed in the list. If not all the polygons are sampled before the maximum number of unique values in the list is hit, a warning message appears on the dialog next to the list.



The purpose of these settings is to limit the use of the field value list for very large datasets with thousands of records. In these cases, it is better to use the 'By Pointing' method to select polygons from the map layer.

Selection Layers

Selection layers are subsets of a feature layer that share the same dataset. When performing many queries, selection layers can quickly overrun a project. Consequently the 'Allow only one selection layer' option, available on the Query Tab of the from the Queries category overwrites the selection layer each time a query or analysis is run.

**Summary Dialog**

The summary dialog opens a window that summarizes the selections made during an OmegaGIS routine. The summary dialog also allows access to saving a query as a cyclical report or threshold alert. On the Query Tab of the Queries category, select the 'Display the routine summary dialog' option to turn this dialog on. The summary dialog does interrupt the routine, so turning it off saves time.

Attachment A

Routine summary

Attribute Query

What?

Layer: 2003 Part 1 Crimes
Query: (ASSAULT)

When?

Dates: 10/1/2003 - 10/31/2003
Times: 06:00 - 12:00
Days: All Days

Registered Types

When a data layer is used in an OmegaGIS routine it should be registered with a type. Registration is possible using the OmegaGIS [MetaData Editor](#) available in ArcCatalog. To avoid populating OmegaGIS routine layer lists with layers that should not be part of queries or analyses, the Queries category provides a Registered Types tab with a setting called 'Only use registered layers'. This option can be set to show only those layers that apply to the specific registered layer types selected.

? Settings for the results of OmegaGIS routines.

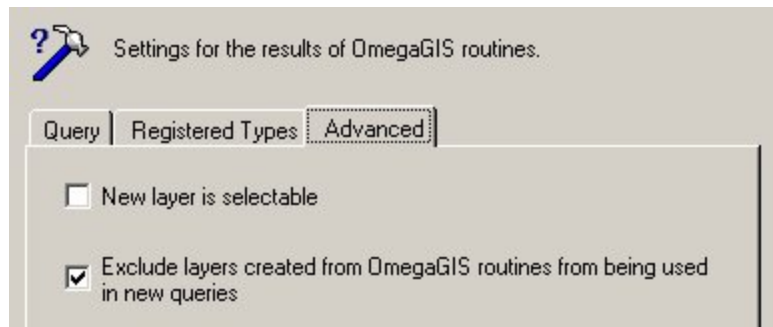
Query Registered Types Advanced

Only use registered layers to make new queries

- Incident
- Person
- Student
- Other

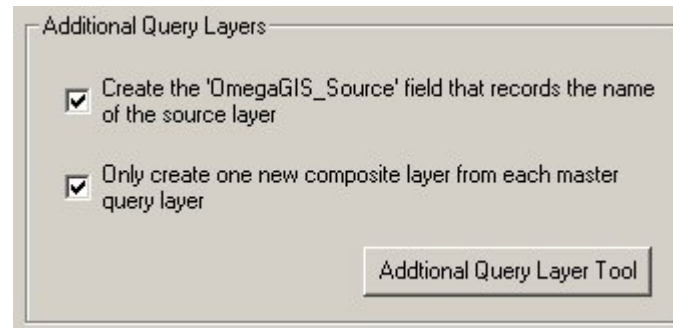
OmegaGIS Layers

As well as explicitly excluding non-registered layers from the layer lists during OmegaGIS routines, layers created by OmegaGIS routines can be excluded from the layer lists. Within the Queries category, on the Advanced tab, the 'Exclude layers created from OmegaGIS routines' can be checked in order to limit layers to be used in analyses to the original data sources and not the output from those sources.



Composite Layers

Composite layers are created when the 'Use Additional Queries' checkbox is used during an OmegaGIS routine. This feature combines query layers during the analysis, and outputs a resulting 'composite' layer. Similar to 'Selection' layers, if a composite layer is created each time a routine is run, the project can quickly become overrun by resultant layers. From the Queries category, Advanced tab, the 'Only create one new composite' option can be selected to overwrite the single composite layer each time a new routine is run.



Map Thumbnails

Map thumbnails are overview images representing the GIS content of a project. From the Advanced tab of the General Settings in OmegaGIS Setup, a thumbnail can be created when the project is closed. Although thumbnails can present valuable overview information while browsing GIS projects in ArcCatalog, creating them automatically while closing a project degrades performance.

Splashscreen

The OmegaGIS splash screen opens during the startup of a project. The image can be turned off to save time. When the splash screen is visible, processing is interrupted to show the image. Turning the image off, allows processing to continue and increases performance.

OmegaGIS Tuning

This section outlines some best practices to improve performance when using OmegaGIS routines.

[Saved Query Database](#)

[Compressing Personal Geodatabase](#)

[Spatial and Attribute Queries](#)

Saved Query Database

The saved query database is responsible for housing queries that are used on a regular basis. The database provides the data source for the [Saved Queries Tree](#), located on many of the OmegaGIS routine dialogs. When a new layer is selected during an analysis, the Saved Queries Tree is populated with all of the saved queries from the database. It is important to keep the number of saved queries reasonable, to reduce the hit on performance while selecting a new layer with associated queries. Databases containing thousands of records can cause a significant reduction in performance as opposed to those with hundreds of records.



A way to limit the number of saved queries is to have one saved query database (Omega_Query.ODB) that contains the most commonly used saved query groups, such as RMS, and place this database in the [project workspace](#). Then have another saved query database that has more detailed saved query groups, such as RMS_Detailed and place this database in a folder other than the project workspace. When it is necessary to use the detailed saved query group, add the path to the database in the OmegaGIS Setup dialog. Note, in this example, the layer would have to be registered to both RMS and RMS_Details saved query groups and the Saved Queries Tree would only be populated with the saved queries groups that were found.

Compressing Personal Geodatabase

Many of the intermediate temporary files created by OmegaGIS are stored in personal geodatabases. In most cases, these databases are compressed when exiting the project. Compressing the databases is important because as they are used, they may become fragmented on disk, taking up more space than is necessary. The Threshold Alert database is the only database that is not compressed automatically. Within OmegaGIS Setup in the Threshold Alert category, an option exists to compress the database.

Attachment A**Spatial and Attribute Queries**

Often GIS layers can be extremely large. Sub-setting the data by using attribute or spatial queries while running an OmegaGIS routine can save significant amounts of time. Where possible, it is important to use the options available from the routine dialogs to subset the data by geographic boundary, time span or particular attributes.

About the Dashboard

Availability by Extension

CrimeView	FireView	School Planner
Dashboard	Dashboard	Not Available

The Dashboard is an extension to Omega Desktop which provides the ability to publish analytical results to a web browser for distribution. The Dashboard extension is new at Omega Desktop 4.3, and can be licensed once Omega software is installed on a machine.

Dashboard content is created within Omega Desktop software, and once created can be automated so that the Dashboard is updated on a regular basis. Omega routines including all query routines, density routines, and the Response Time Map routine in FireView are available for automating content to the Dashboard. The results of all other routines can be posted to the Dashboard as maps or reports by using a publishing tool provided with the software.

It is important to consider hardware, software and personnel when determining the best approach for setting up the Dashboard. A desktop machine must be identified that will run Omega Desktop software, as well as a web server and a database server. The web server will host two web applications; one for viewing the published data, and one for managing the data. In addition, a web service running on this server will provide the means for moving data from the desktop machine to the web server. The database server will provide a repository for storing metadata about the information that is posted. Finally, it is necessary to identify the personnel that will be responsible for managing the Dashboard application.

Omega Dashboard Login - Windows Internet Explorer

http://www.omegashboard.grp/lincoln/dashboard/login.asp

File Edit View Favorites Tools Help

Omega Dashboard Login

Lincoln Police Department

LINCOLN
The Community of Opportunity

Welcome to the Lincoln Dashboard!

This site provides command staff with a selection of graphic views of crime data in their jurisdictions: current incident and thematic maps, comparison maps, graphs, crime reports and a collection of relevant web sites and documents. The application, represented in viewer panes, displays crime data:

- by different geographic areas (eg: beats, city etc...)
- by timeframes (eg: hour/day/week)
- by types of crimes (eg: part 1 only) or by any requested variables from the source database

Contact Lincoln to customize a page that provides the information you need to prepare reports, make presentations, analyze trends and assist with tactical and strategic decision making.

LOG IN

User Name:

Password:

Login

Hardware Requirements

The Dashboard is a very lightweight software product which can take advantage of a department's existing server architecture, as long as those servers are within the Local Area Network (LAN). A department server structure may include both a web server and database server, or just one server running both database and web applications. The database server must have SQL Server 2005 or SQL Server Express installed, the Web Server must have IIS 6.0 and .NET Framework 2.0 installed.

One recommendation to note is that a server used as a Domain Controller by an agency should not be used to host the Dashboard web applications database. A Domain Controller can be recognized by the fact that it is running Active Directory; a component used to control user names, passwords and permissions to all machines within the network.

Using Existing Hardware

If a department has an existing Database Server running SQL Server 2005 or SQL 2005 Express, the database component of Dashboard can be installed. The initial size of the SQL database is only 2Mb. 100 Mb of space on the Database Server is sufficient to ensure that data has plenty of room to grow as content is added to it.

If a Web Server is already set up, the Dashboard can be installed on the existing server. The Web Server will require a shared folder be created on disk to store all of the files that are posted from CrimeView or FireView up to the server. These files consist of .PDF and .JPG formats, and may vary in size from 100kb to 1Mb depending on the file. 5 GB of space on the Web Server will ensure there is plenty of room for the Dashboard content to grow. For example, a web server with about 400 files published to the server might take up about 300 Mb of space.

Workstation Option

If for some reason an agency does not have existing servers available, or they are outside of the LAN network, then new hardware will need to be purchased. For a small department, it is possible to purchase a Workstation instead of a Server, however the Workstation will eventually need to be upgraded to a Server if the agency opts to upgrade the Dashboard to receive content from ArcGIS Server.

Single Server Option

An upgrade to the Workstation Option is purchasing a single server that acts as both the Database Server and the Web Server. This server has SQL Server 2005 or SQL 2005 Express installed as well as IIS 6.0 to run the web applications. The drawback to this configuration is that SQL Server can slow down the web applications. However, for a small department this limitation is negligible. The following minimum specifications are recommended for this server:

- 4 GB RAM
- Dual Dual-Core Intel Xeon Processors (3.0 Ghz or higher)
- RAID 1 and RAID 10 Disk Configuration using SAS discs 15K RPM (6 discs total)
- 1 Gigabit Ethernet network cards

Multiple Server Option

Attachment A

In a larger agency, it is standard practice to separate the Database Server from the Web Server. If an agency is interested in this configuration, the Server specification above should be used as the Database Server, and the following specifications should be used for the Web Server.

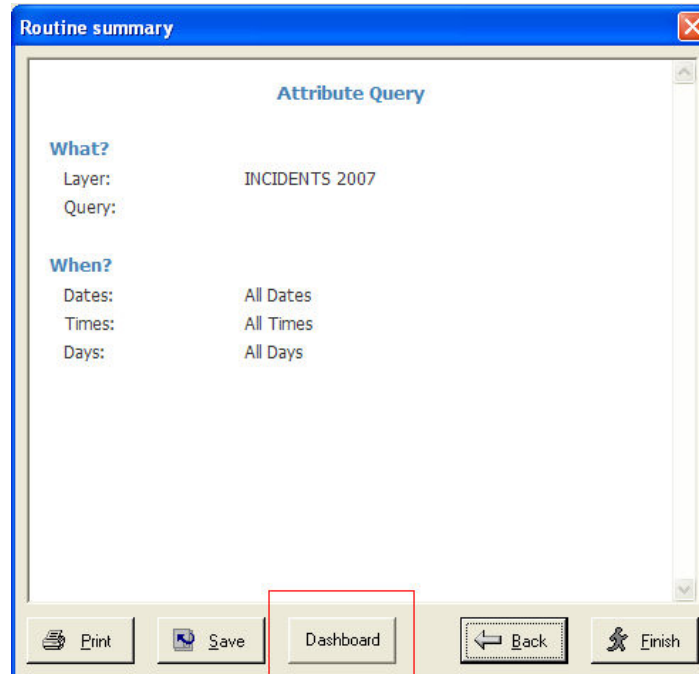
- Dual Dual-Core Intel Xeon Processors (3.0 Ghz or higher)
- 4 GB RAM
- RAID 10 Disk Configuration using SAS discs 15K RPM (4 discs minimum)
- 1 Gigabit Ethernet network cards

The Dashboard Wizard

Introduction

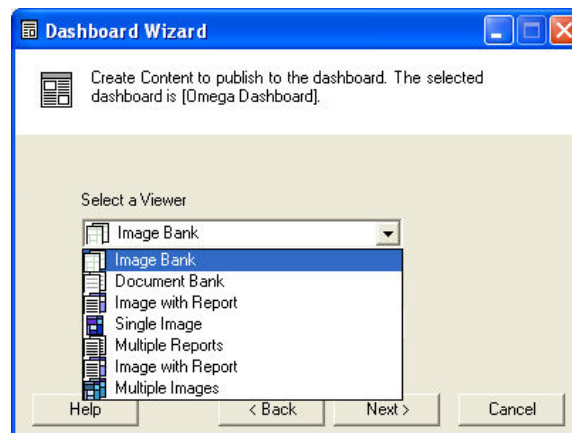
The Dashboard Wizard is embedded in the Query, Density and Response Time Map routines of Omega Desktop software. The Wizard provides a way to save the results of these routines to a server, which can then be viewed using a web browser that displays the Dashboard application. To access the Dashboard publishing capabilities from these routines, simply configure Omega Setup to open the Summary dialog before the routines are run. A 'Dashboard' button on the Summary dialog will open the Dashboard Wizard.

Before using the Dashboard Wizard it is important that the Dashboard Administrator create the Viewers that will be used to group the published results. Viewers are the building blocks of the Dashboard, and each Viewer represents one panel on the Dashboard Viewer web site that can be displayed through an internet browser. Results may only be posted to predefined Viewers, and Viewers can not be created from the desktop application. To discover how to create Viewers, see the Omega Dashboard Administrator help guide.



Dashboard Wizard Dialogs

When the Dashboard Wizard is opened, the first panel that is presented enables the ability to select from a list of Viewers that have already been created by the Dashboard Administrator. If the Dashboard Administrator has not created any Viewers, there will be two Viewers available by default; the Image Bank and the Document Bank.



Attachment A

The Image Bank can be used to store maps or graphs published from the Wizard, while the Document Bank may be used to store any reports that are created with the Dashboard Wizard. Other Viewer types that may have been created by the Dashboard Administrator will be listed, and the various Viewer types can be identified by the icon that is displayed with the Viewer name. The Viewer types are listed below with their icons.

Single Image

A Single Image Viewer stores an image and presents it as a panel on the Dashboard. With the Wizard, a map or graph can be created and saved to the Viewer.

Multiple Images

The Multiple Image Viewer builds upon the Single Image Viewer in that more than one map or graph can be added. When viewed on the Dashboard, the user is able to scroll through the images in an accessible manner.

Image with Report

In this viewer, a map image is always linked to a report. Similar to the Multiple Images Viewer, the user can scroll through the images, but in addition, a link to a report for each image is included.

Reports

The Report Viewer presents a list of report links. The user can click on any of the links in order to view the report in PDF format.

Image Bank

The Image Bank is simply a Multiple Image Viewer with a specific name. This Viewer is designated as the default Viewer for all images that are published with the Dashboard Publisher tool.

Document Bank

The Document Bank is a Reports Viewer with a specific name. This Viewer is designated as the default Viewer for all reports in PDF format that are posted using the Dashboard Publisher tool.

***MyLinks**

An additional Viewer type called MyLinks is available when viewing Dashboard content through a browser. This type is not available from the Desktop Dashboard Wizard however as it does not involve generating content from the desktop application.

Content Type

Once a Viewer is selected, a content type may also be selected from a dropdown list. Only certain content types are available to certain Viewers. For example, the Document Bank Viewer may only receive 'report' type content, and so, only the Report type is listed in the Content Type dropdown list. If the Image Bank Viewer is selected, only content that can be produced as an image is listed, and so, a map or graph content type is listed in the dropdown list. Selecting the Viewer will predetermine the type of content that is available and may be published to that particular Viewer.

Name and Description

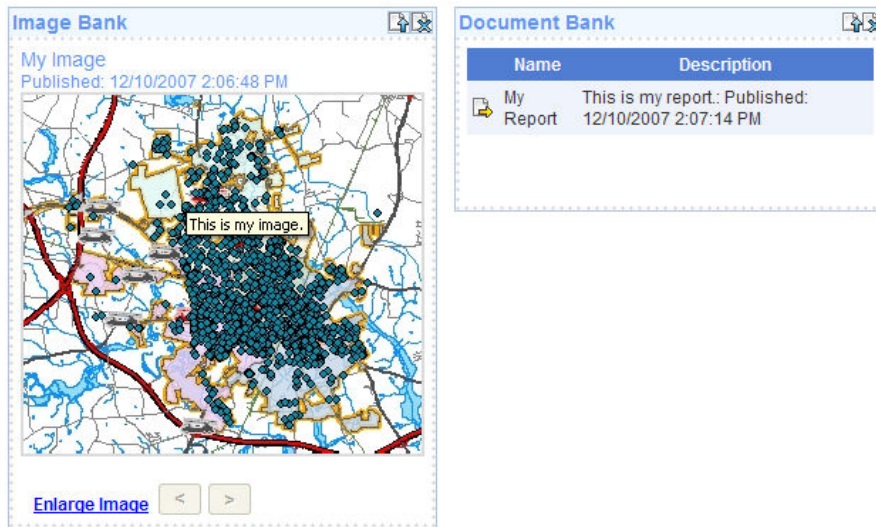
After clicking the 'Next' button a new panel will appear that offers the ability to save a name and description for the content to be pushed to the server. A name must be entered into the textbox, however the description is optional. Click the next button to proceed to the next panel in the Wizard.



The screenshot shows a window titled "Dashboard Wizard" with a blue title bar. Inside the window, there is a header area with a small icon and the text "Enter a name and description for the content." Below this, there are two text input fields. The first is labeled "Enter a Name" and contains the text "New Map". The second is labeled "Add a Description" and contains the text "This is a new map". At the bottom of the window, there are four buttons: "Help", "< Back", "Next >", and "Cancel".

The content name that is entered will be visible in the first line on the Viewer panel, while the description is accessible based on the type of content that is published. For instance, if a map or graph is published, the description can be accessed by hovering over the image, but if a report is published, the description is located next to the report name. An example of the location of both name and description are provided below.

Attachment A



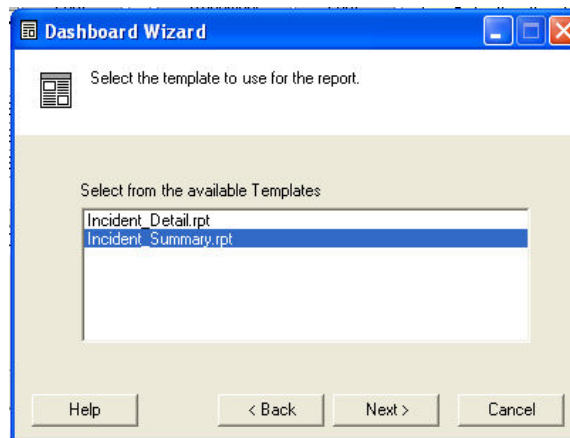
Templates

The next panel that will appear on clicking the 'Next' button will depend on the type of content that is published, but in all cases a panel is presented that allows for the use of particular templates to be associated with the content produced. If a map type is selected, then a template panel for Map Layouts is presented, if a Report or Graph type is selected, then a list of report or graph templates will become visible. If the Image with Report content type is selected, the Map Layout template panel is presented after which time the 'Next' button can be used to move to the template panel for the report that will be associated with the map.

Report Templates

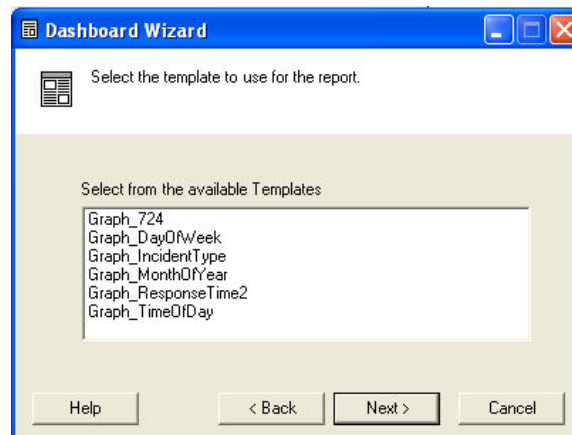
Report Templates are provided with the Omega Desktop software and are customized to show detailed information about incidents that are selected by Query analyses. Crystal Reports is used to create these templates and the files are stored in a standardized project folder called \Reports. The files stored in this folder are automatically found by Omega Desktop software, including the Dashboard component, however to store reports in an alternate location Omega Setup can be used to identify the new location of the reports.

Once the report templates are created, they must be registered to the corresponding incident layers using the Omega Metadata Editor available on the Omega Data Management extension of ArcCatalog. Once the report is registered to the incident layer, it will appear in the template dropdown list of the Dashboard Wizard.



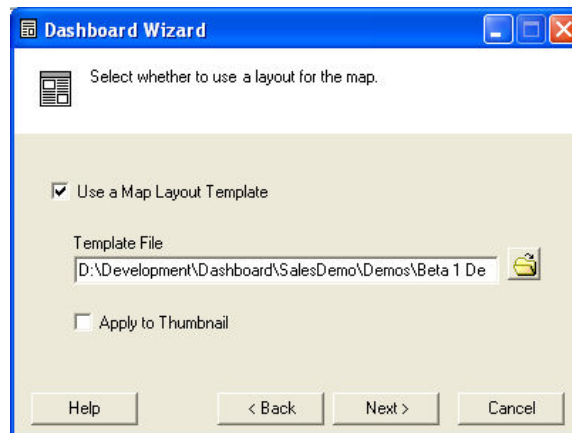
Graph Templates

Graph templates are provided with Omega Desktop software, and can be located in the Omega Desktop installation folder under the folder \graphs. Any graph that is located in this folder will be picked up by the Dashboard Wizard and displayed in the graph template list. New graph templates can be created and used by the Dashboard Wizard as long as they are located in this folder.

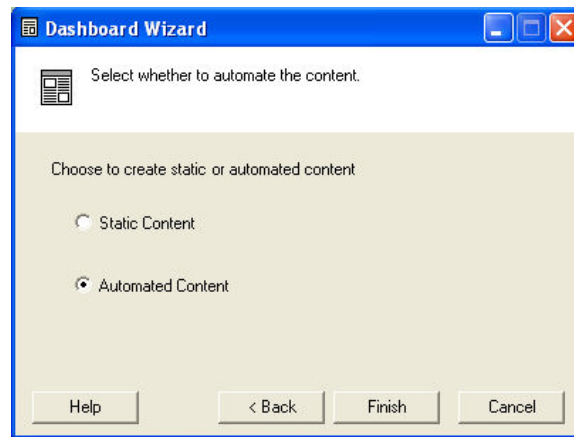
Attachment A**Map Templates**

If a map content type is selected, an option exists to create the map with a page layout. The page layout is used to add elements to the map such as a legend, scale bar, north arrow and disclaimer. Page layouts are created using ArcMap, and this file can be selected using the Dashboard Wizard, and the map will be posted with the page layout.

An additional option called 'Apply to Thumbnail' is provided so that the page layout can either be attached to the map thumbnail or disregarded. When an image is posted to the server, both a large size and a thumbnail are created. The thumbnail is the image that is presented on the Viewer panel when it is displayed within the Dashboard Viewer website. In some cases, adding the page layout to the thumbnail may prevent the map from being clearly legible which is the reason for omitting it from the posted thumbnail image.

**Automation**

The final step in the Dashboard Wizard involves identifying whether the content will be posted as static or as automated. If the content is posted as static, then it will not be able to be updated on a regular basis. This content will be posted only once to the server. If the Automated content option is selected, the content may be set up to run regularly. The date duration must be selected from a list to identify which time period will be selected when the automation is run.

Attachment A

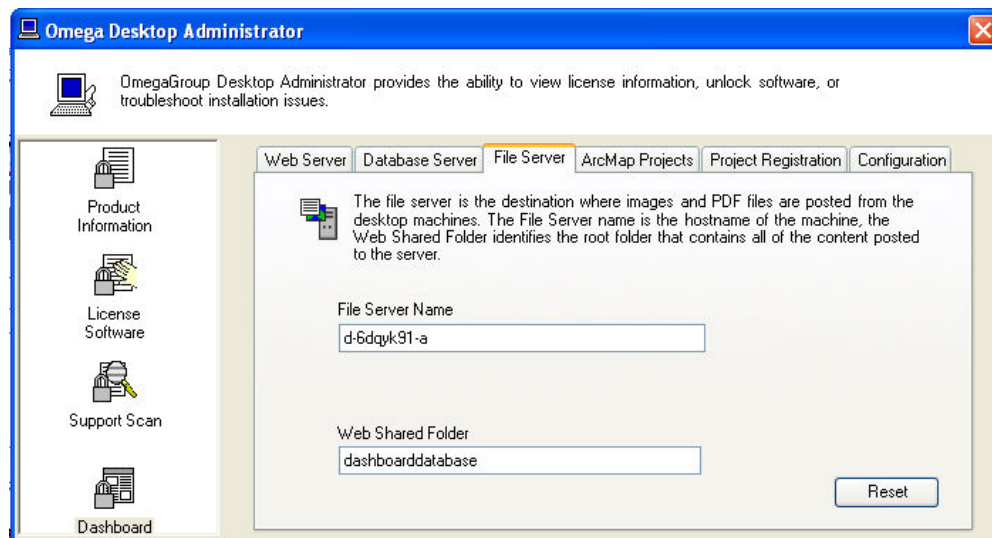
Clicking the Finish button will post the results to the server. All individuals that have been granted permission to view the results in the Dashboard Viewer website will be able to see the posted data whether it be maps, reports or graphs within one of the Viewers created by the Administrator.

Where Is the Data Posted?

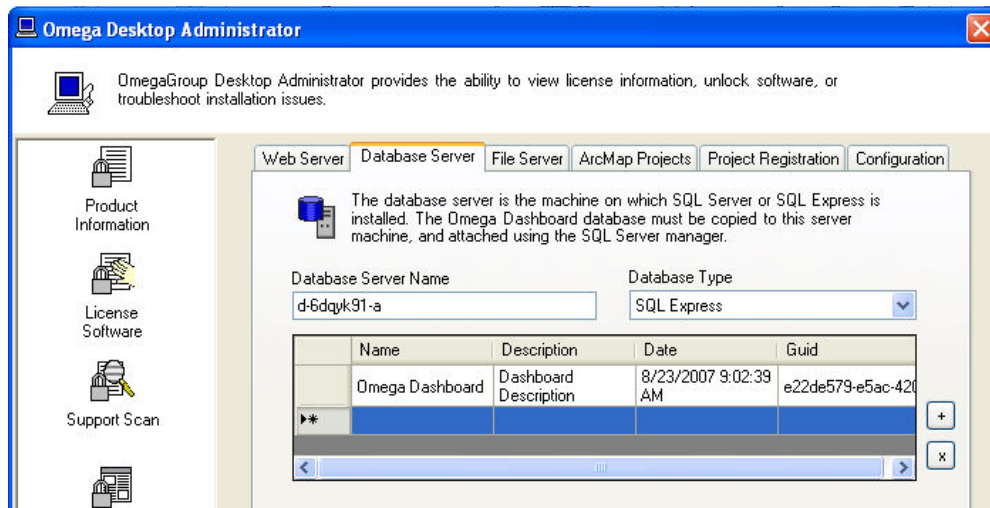
When data is posted, it is the Omega Desktop Administrator that determines where this data will be delivered. The data is posted to one or more servers where it is stored for future use. Different agencies will have different server architectures, but there may be a maximum of three servers that can be used to store data.

The File Server

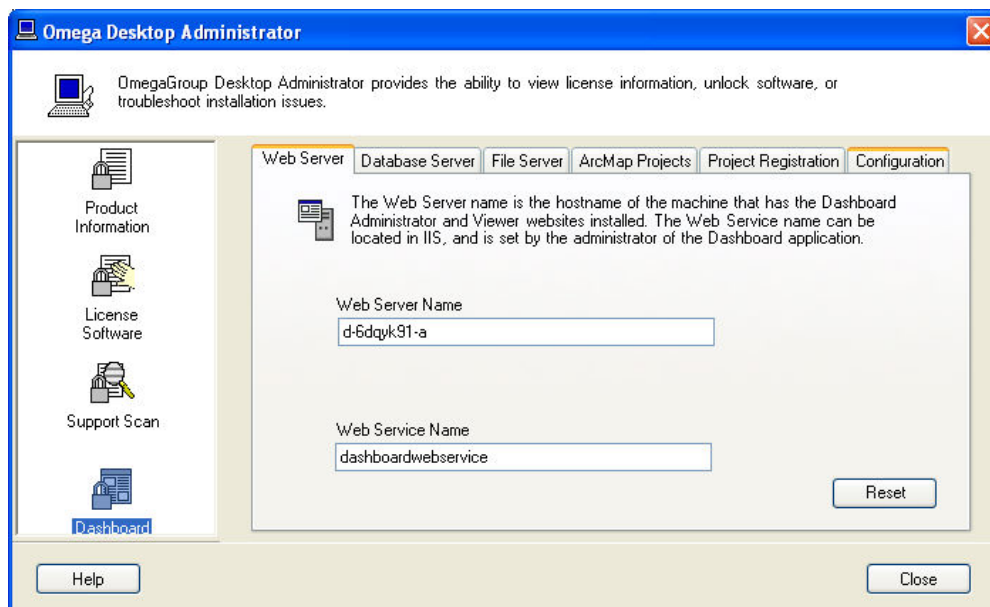
The file server is where the image and PDF files are sent when they are posted from the desktop using the Dashboard Wizard, Dashboard Publisher or Dashboard Editor. The file server information is identified in the Omega Desktop Administrator within the Dashboard Category on the File Server tab. The name of the file server and the name of the Web Shared Folder can be determined from this tab. The Web Shared Folder is created by the Dashboard Administrator personnel. This folder is shared so that both the Dashboard Viewer and Dashboard Administrator websites can access the data.

**The Database Server**

The database server is the machine on which SQL Server 2005 or SQL Server 2005 Express is installed by the Dashboard Administrator personnel. The SQL Server software manages a SQL database called OmegaDashboard which can be placed in any folder on the database server. Information pertaining to the database server settings can be collected using the Omega Desktop Administrator, Dashboard Category, Database Server tab.

Attachment A**The Web Server**

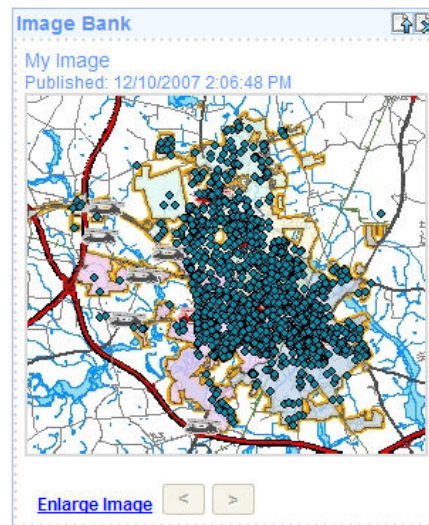
The web server is the location where the Dashboard Viewer and Administrator websites are run. The web server must have IIS 6.0 installed to run the websites. To determine information about this server the Omega Desktop Administrator, Dashboard Category, Web Server tab can be used. In addition to the websites, the web server also runs a web service that is used in the communication between desktop and server machines. This web service can be identified on the same tab.



In many cases, the data files, the database and the websites can all be located on the same server. As long as the server has SQL Server 2005 or SQL Server Express 2005 and IIS 6.0 installed, one server machine can be used to run all server components of the Omega Dashboard.

What Is Posted to the Server?**File Types**

When data is posted to the server, it may be posted as a few different types such as maps, reports, graphs or pictures. Maps, reports and graphs may be published using the Dashboard Wizard or Dashboard Editor. If the type is a map or graph, these files are actually posted twice, as a thumbnail image, and as a larger sized image. The thumbnail image is what is used on the Dashboard Viewer website to show an immediate view of the map or graph within a Viewer panel. Notice in the image below that the map shown is the thumbnail image posted to the server.

Attachment A

The larger sized image is displayed once the 'Enlarge Image' option is selected on the panel. The size of this larger image is determined by the screen resolution on the desktop machine that was used to publish it. Depending on the screen resolution, the image will be created at a size that will always fit within the same screen resolution on a browser.

If the file type is a report then the file is posted again to the server, but this time only one file is posted in a PDF format. These files types are available for viewing within a Reports list. In the example below, a single report has been published to a Multiple Report Viewer. Clicking the yellow arrow to the left of the report name, will open the report PDF file in a new browser window.

Name	Description
My Report	This is my report: Published: 12/10/2007 2:07:14 PM

Any image in JPG format or document in PDF format may be published to the server using the Dashboard Publisher tool. These files are posted in the same way in that the image file is posted as a thumbnail and at an enlarged size, while the document is posted once as a PDF.

Obtaining the Best Results**Publishing Maps**

There are a few considerations to take into account when publishing maps to the server. When publishing image files to the server, it is important to consider the screen resolution which a majority of the personnel will be using on their machines. If for instance, if images are published at 1280 x 1024, but most users are viewing the information through their browser at 1024 x 768, then they will have to use the mouse to expand the images in order to view the entire file. When publishing imagery, it is recommended that your screen resolution match that of the majority of users accessing the Dashboard Viewer website.

If in addition to publishing the map, a page layout is included it is important to create the page layout at the same screen resolution that will be used to publish the map. If for instance a screen resolution of 1280 x 1024 is used to create the page layout, but the map is actually published at 1024 x 768, the resulting layout will appear blurry as it is compacted during the publishing process to fit the screen size.

Publishing Pictures

Images other than maps may be posted using the Dashboard Publisher tool. When posting an image, it is a good idea to ensure that the image is smaller than the screen resolution. To be safe, publishing the picture at 65% of the size of the screen resolution will ensure that the picture does not need to be expanded when it is viewed through the Dashboard Viewer website. For instance, a picture published at 1024 x 768 should be no larger than 666 x 499 in size.

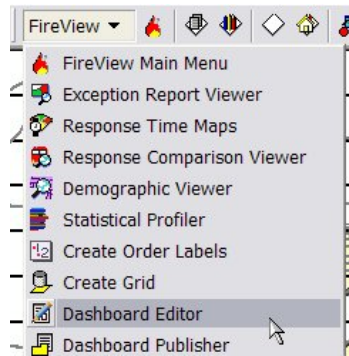
Publishing Documents

Documents are published in PDF format, and so a consideration of the size of the document is necessary when determining if a report is suitable to be viewed through the Dashboard website. Large sized documents will take longer to open.

The Dashboard Editor**Overview**

Attachment A

The Dashboard Editor manages data that has already been published to a server to be displayed by the Dashboard Viewer. To review, the Dashboard Viewer is a website that provides the ability to view data published from Omega Desktop through Internet Explorer provided that they have the appropriate permissions. The Dashboard Editor tool can be accessed from the FireView or CrimeView dropdown menus.



Once opened, the Dashboard Editor loads all of the data that has been published to the server from the current ArcMap project into a tree that is located on the left side of the dialog. Depending on the network connection, loading the dialog may take a few moments as the data is being retrieved from a server. It is important to remember that the only information displayed within the dialog is that data that was generated with the current ArcMap project.

Dashboard Editor Dialog

On the right side of the dialog is a panel that contains detailed information about the node that is selected in the tree. When the dialog first opens, this information will describe the project that is currently open in ArcMap. The descriptive information provided is outlined below:

Project Name

The name that was entered using the Omega Desktop Administrator when the project was registered to the Dashboard.

Description

The description that was entered using the Omega Desktop Administrator when the project was registered to the Dashboard.

Dashboard Host Server Name

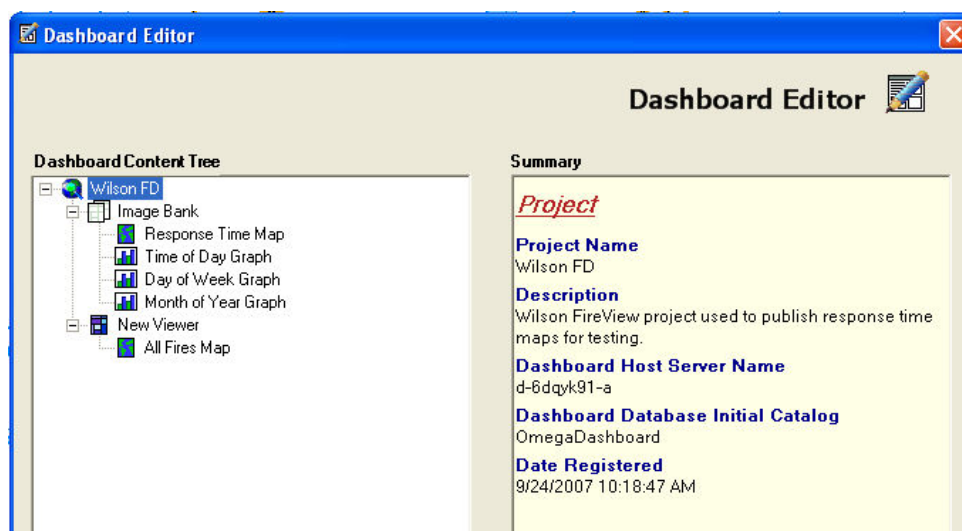
The name of the server that is currently hosting the Dashboard SQL Server database.

Dashboard Database Initial Catalog

The Dashboard Database Initial Catalog is the name that was used when the database was attached to SQL Server.

Date Registered

The date that the project was registered to the Dashboard using the Omega Desktop Administrator.

**Dashboard Viewers**

Clicking on the '+' icon to the left of the Project node will expand a list of Viewer nodes within the second tier of the Dashboard Editor tree.

Attachment A

Viewers are categories that are created with the Dashboard Administrator in order to group data together into logical units. The personnel responsible for administering the Dashboard must create these Viewers before the Dashboard Editor can be used. Only those Viewers that contain data that was published with the current ArcMap project will be visible within the Dashboard Editor.

Viewer Icons

Different types of Viewers are available in order to show different groupings of data. These types can be distinguished within the tree by their icon that is associated with the Viewer text. In addition to the icon displayed in the tree, hovering over these icons will display the Viewer type as well. The Viewer types are identified below:

Single Image

Viewer supports posting only one image.

Multiple Image

Viewer supports posting multiple images.

Image and Report

Viewer supports posting one map and an associated report.

Multiple Reports

Viewer supports posting multiple reports.

Image Bank

Viewer used with the Dashboard Publisher to house images, but can also receive content from the Dashboard Wizard.

Document Bank

Viewer used with the Dashboard Publisher to house documents, but can also receive content from the Dashboard Wizard.

**Dashboard Content**

Dashboard content refers to data that is posted to the server from the Dashboard Publisher or Dashboard Wizard tools that are used within the Omega Desktop products. The Dashboard Editor will only display content that is published to the server with the Dashboard Wizard. This limitation is due to the fact that the Content Editor can only be used to modify content that is generated within the currently opened and registered ArcMap project.

There are several types of content, and these types can be distinguished using the icons that are placed next to the content text within the tree. The types can also be identified by hovering the mouse over the content icons. The types of content available to the Dashboard Editor are outlined below:

Map

A map can be generated using the Dashboard Wizard which is launched from the Summary dialogs of the Query, Density or Response Time Map routines.

Map with Report

A map with report type is generated using the Dashboard Wizard. When viewing this content within a browser, the map and report are always linked.

Graph

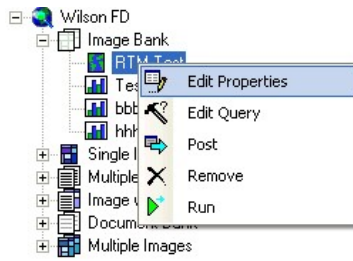
Graphs are also generated with the Dashboard Wizard. The graphs that are available depend on the graph templates that are stored in the OmegaGroup installation \graphs folder.

Report

A report is generated with the Dashboard Wizard. The reports that are available will be those reports that are registered with the incident layer that is selected by the Query, Density or Response Time Map routines.

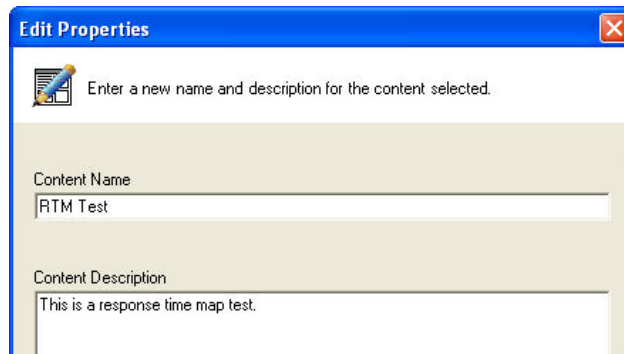
Editing Options for the Dashboard Editor

There are five options that are available to the Dashboard Content. These options can be viewed by right-mouse clicking on a content item within the tree. The options are outlined below:



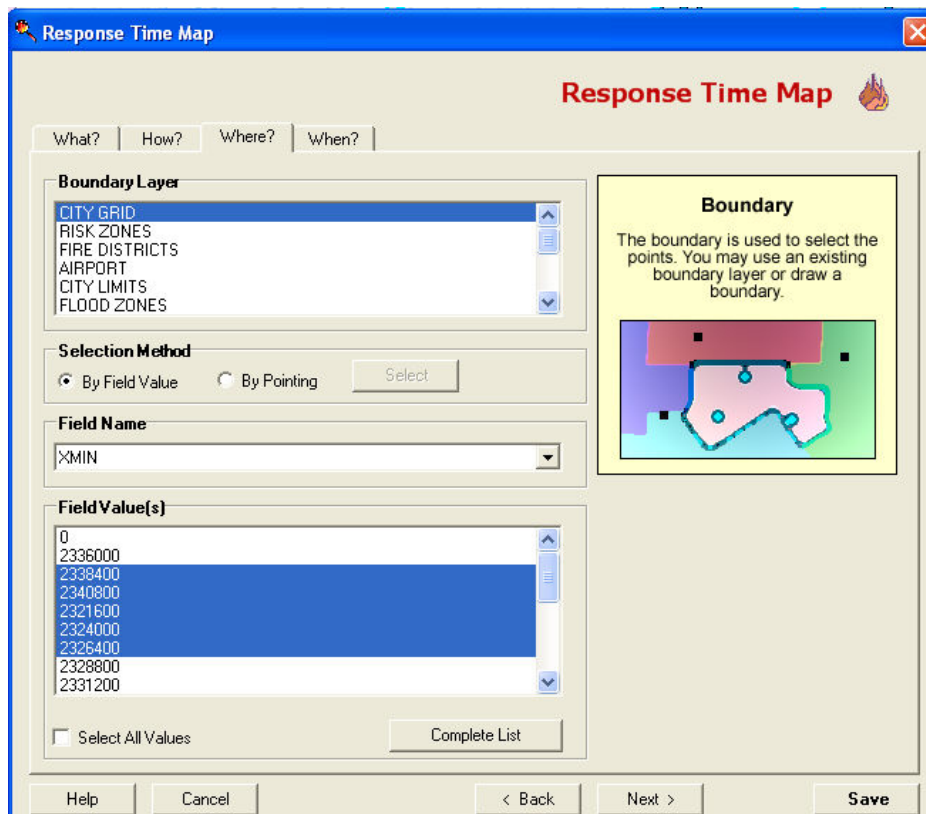
Edit Properties

This option opens a new dialog which will load the current name and description for the content item selected. After entering a new name and description, the text on the Dashboard Editor will be updated to reflect the changes. These changes do not take effect until the content is posted to the server.



Edit Query

Edit Query opens up the original analysis dialog so that the query that was used to select the incidents can be changed. Clicking the 'Save' button on the analysis dialogs will save the new query to the project XML file within the project workspace. The content is not updated with the new query, until it is posted to the server.



Attachment A**Post**

Posting the content to the server saves the property and query edits, and updates the changes on the server. The data is posted both to the SQL Server database as well as updating the images or documents that are stored on the server. Posting content changes will run the analysis in order to recreate the results as a map, graph or report, whatever was specified originally when the content was first created.

Remove

Remove will delete the content from the server by removing the record in the SQL Server database that is associated with the content, as well as removing any stored images or PDF files on the server.

Run

This option runs the selected content to regenerate the report, map or graph that is selected. This option can be used if edits are made to the property or query in order to view the results without posting the changes to the server.

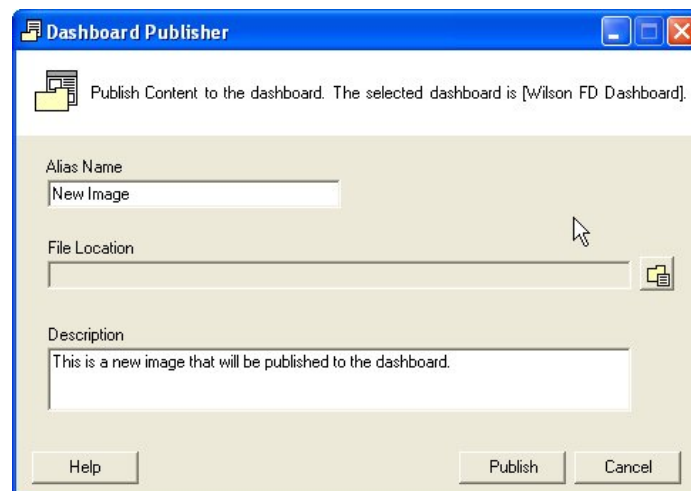
The Dashboard Publisher**Introduction**

The Dashboard Publisher tool allows the analyst to select a file that is saved in PDF or JPG format and post that file to the Active Dashboard on the server. The Active Dashboard is defined as the dashboard that is currently receiving content from the desktop machine. This setting is configured using the Omega Desktop Administrator. The Dashboard Publisher is available to all desktop machines that have been licensed with a Single License of Dashboard.

Content that is posted to the server using the Dashboard Publisher is published one time and cannot be automated. Once the content is posted, it cannot be deleted from the desktop machine, but must be accessed by the Dashboard Administrator through the Dashboard Administration website.

When content is published, metadata including the alias name, description and date published are posted to the dashboard database, while the file (PDF or JPG) is saved to disk on the server. When the data is published, it is automatically routed to the 'Report Bank' and 'Image Bank' Viewers. Viewers are organizational tools that allow the Dashboard Administrator to organize content as it is posted. In this case the 'Report Bank' and 'Image Bank' Viewers are designed to receive either PDF reports or images that are published through the Dashboard Publisher tool.

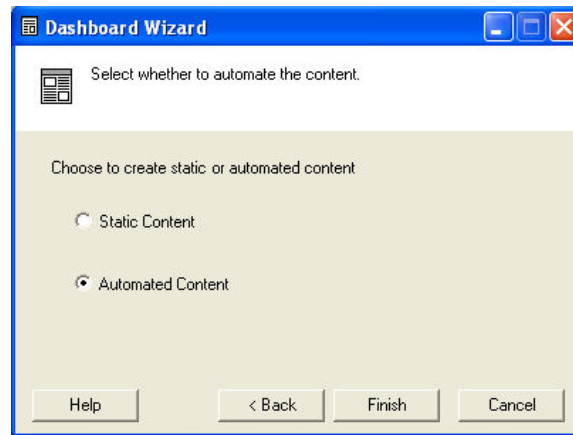
When using the Dashboard Publisher, note the location to which the content is posted within the descriptive panel on the dialog. The Dashboard name is provided within the square brackets. In addition, before the content is published, a message is provided that indicates where the content will be posted. Once posted, the Administrator of the Dashboard may choose to make the Viewers that hold the content visible to other users or may maintain them as invisible until the content is ported to other visible Viewers.



To use the Dashboard Publisher, select the tool from the Omega Desktop dropdown list in order to open the dialog. Enter an alias name and description for the file, and select the file using the browse button. Ensure that the file type desired is selected at the bottom of the dialog (PDF or JPG). Use the Publish button to post the file to the Dashboard on the server.

Dashboard Automation**Description**

Dashboard Automation is available to the content that is published using the Omega Dashboard Wizard. When the Wizard is used, an option is available that specifies whether the content should be tagged as 'Static' or 'Automated'.

Attachment A

When content such as a map, graph or report is posted to the server as 'automated content', the query used to produce the results is written to the Dashboard database as metadata. The metadata ensures that each time the content is updated, the same query is used. Once content is posted to the server, the Dashboard Administrator web site, can read this metadata to determine which content can be automated. All content tagged with the 'automated' option in the Dashboard Wizard can be assigned to a Job. The Job is then used to automate the content on the desktop machine using Windows Task Scheduler.

Creating a Job

To create a new Job to run the map, graph or report on a regular basis, the Dashboard Administrator web site must be opened to the Job tab. A new Job can be created which allows the administrator to select from a number of ArcMap projects that are currently publishing data to the Dashboard. When a project is selected, a list of automated content that has been published to the Dashboard is then available for selection. When the Job is saved, a new Job Number is created automatically. It is this Job number, that must be used on the desktop machine to set up a Windows Scheduled Task. For more information on administering Jobs, see the Dashboard Administrator help guide.

Attachment A

Dashboard Administrator - Windows Internet Explorer

http://localhost:52424/Dashboard_Admin_Website/DashboardUI.aspx

File Edit View Favorites Tools Help

Dashboard Administrator

OmegaDashboard
ADMINISTRATOR [Logout](#)

Overview Projects Viewers Content Roles Users **Jobs** SMTP Email

Jobs define the Content that will be automatically published from a desktop machine using Omega Desktop software. When a machine is identified, a list of Content that was generated from that machine is populated. Only Content with a type of Automated will be displayed in this list. When a new Job is created, the Job number is used run the automated Content from Windows Task Scheduler on the desktop machine.

Jobs
Repeat Calls Job

Job ID
8

Job Name
Repeat Calls Job

Description
Job created to show all repeat calls of Part 1 Crimes.

Project
LincolnDemo

Automated Content

- Repeat Calls: Assaults Map and Report
- Repeat Calls: Boundary by Field ID
- Repeat Calls: No Boundaries
- Repeat Calls: Selection by Mouse

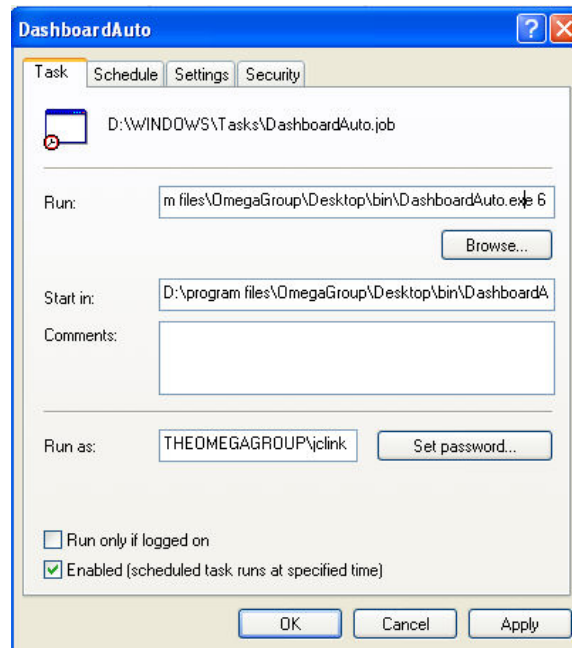
Add Edit Save Remove

Done Local intranet | Protected Mode: Off 100%

Scheduling a Job

Scheduling a Job to run is performed on the machine that initially posted the content. The Job is run from Windows Task Scheduler, and all content that was referenced to the Job number by the Dashboard Administrator will be run if the task is set up for the Job. Scheduling an automated Job is a function of the Dashboard Administrator. For more information, see the Dashboard Administrator help guide.

Attachment A

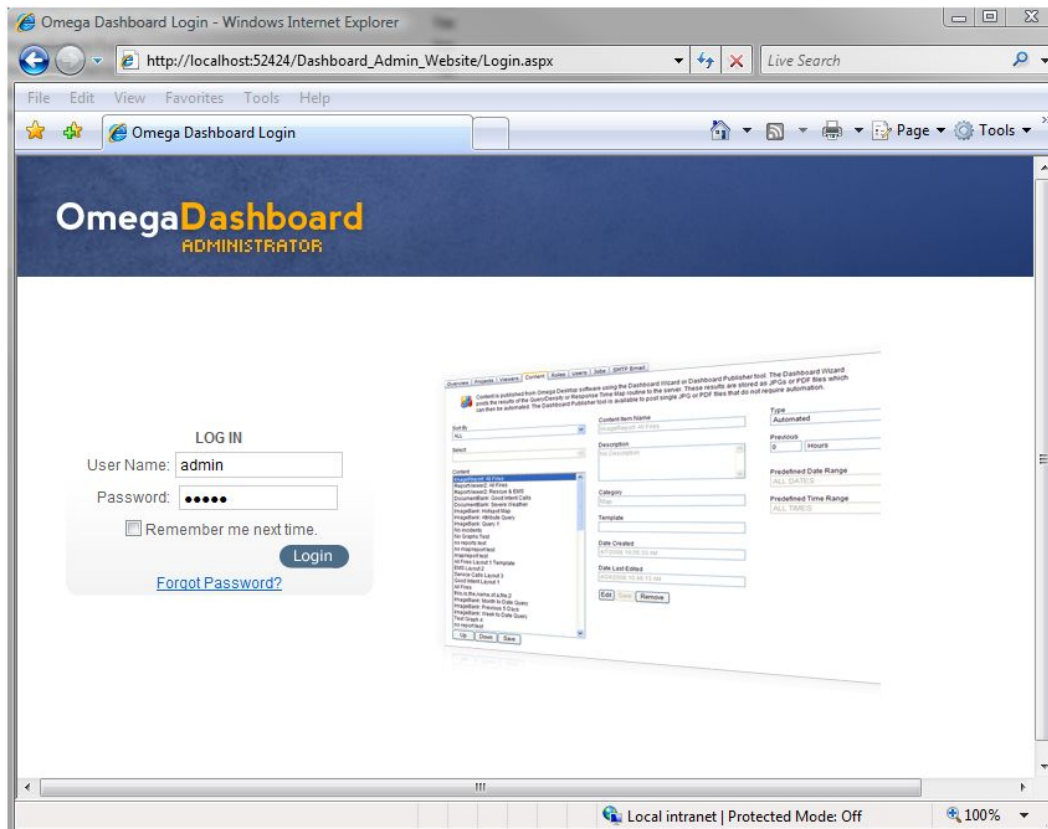


Dashboard Administrator

Introduction

The Dashboard Administrator is a web site that is used to organize the content published to the server from any desktop machines running Omega Dashboard. When content is published to the server, metadata is stored in a database, while the images or portable documents (PDFs) created are stored in a predetermined folder on disk. The Dashboard Administrator, reads the information from the database, and manages the organization of this content both within the database and on disk.

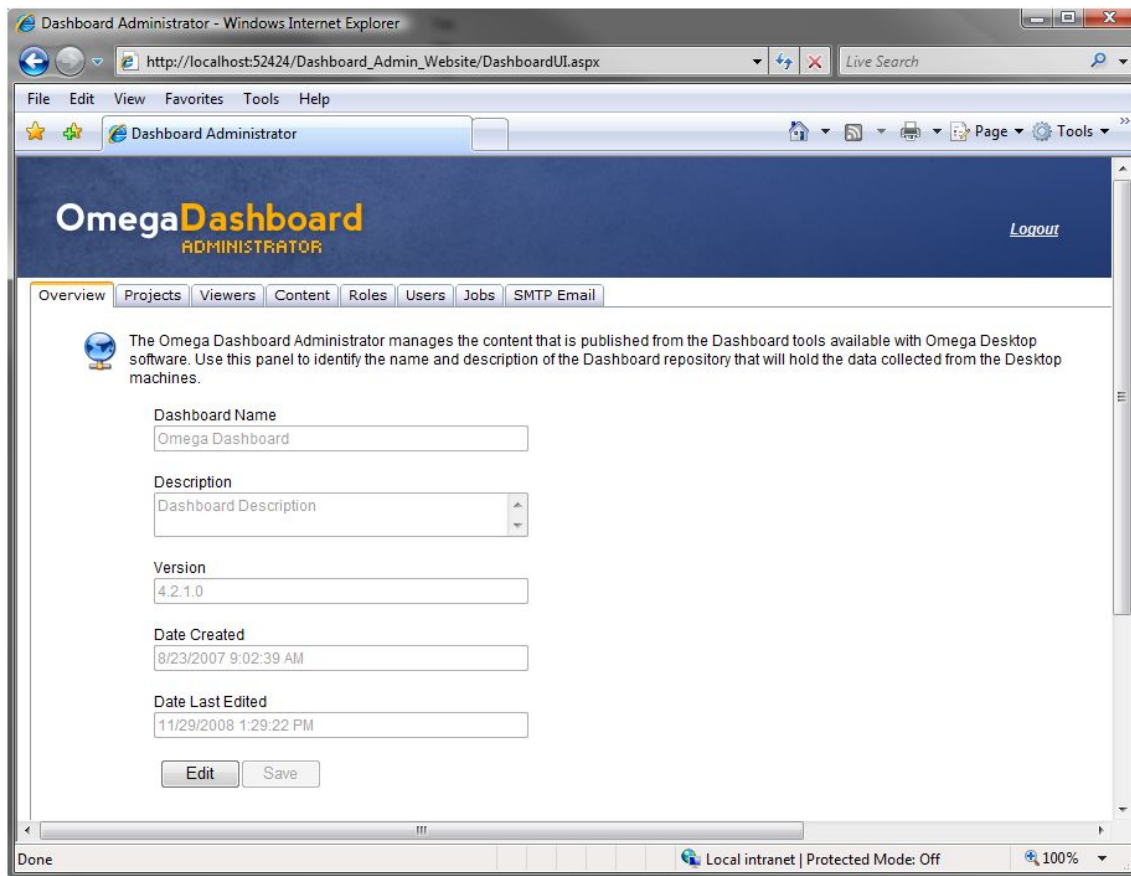
The Dashboard Administrator web site consists of eight tabs. The tabs divide the administration of the Dashboard content into sections for manageability. These tabs are described in the following sections of this help guide.



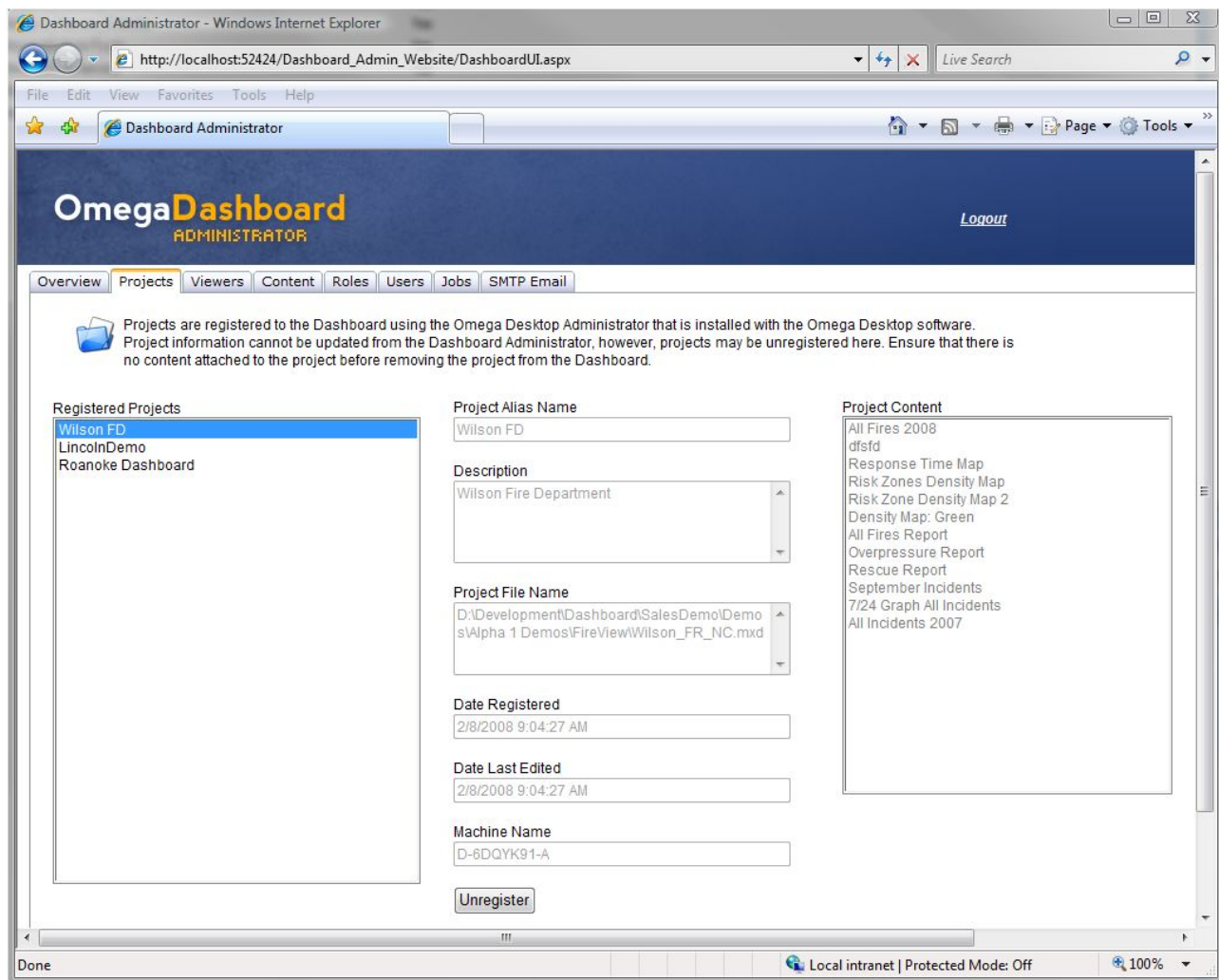
Overview Tab

The Overview tab provides information about which version of Dashboard is running. It is important to take note of the version as it is associated with the ArcGIS version publishing content to the server. If running ArcMap 9.2 on the desktop machines publishing Dashboard content, the Dashboard Version should be identified as 4.2.1. Alternatively, if running ArcMap 9.3, the version of the Dashboard on this tab should be 4.3.0.

The name and description of the Dashboard may be modified by the Administrator from this tab. When either of these items are updated, the date edited will be updated with the date and time that the name and description were modified.

Attachment A**Projects Tab**

The Projects Tab of the Dashboard Administrator displays the ArcMap projects that are registered to the Dashboard. ArcMap projects are registered using the Omega Desktop Administrator. As the projects are registered, the information regarding where the project is located on the desktop machine, and which machine is housing the project is recorded in the Omega Dashboard database. The Dashboard Administrator web site retrieves this information to display it on the Projects Tab.

Attachment A**Projects Tab Layout**

The list located on the left side of the Projects Tab displays the ArcMap projects that are registered to the Dashboard. Projects are registered using the Omega Desktop Administrator. Each of these projects has the capability of publishing content to the Dashboard. Once registered, these projects should not be moved on the machine or relocated to another machine without unregistering and reregistering the project from the Omega Desktop Administrator.

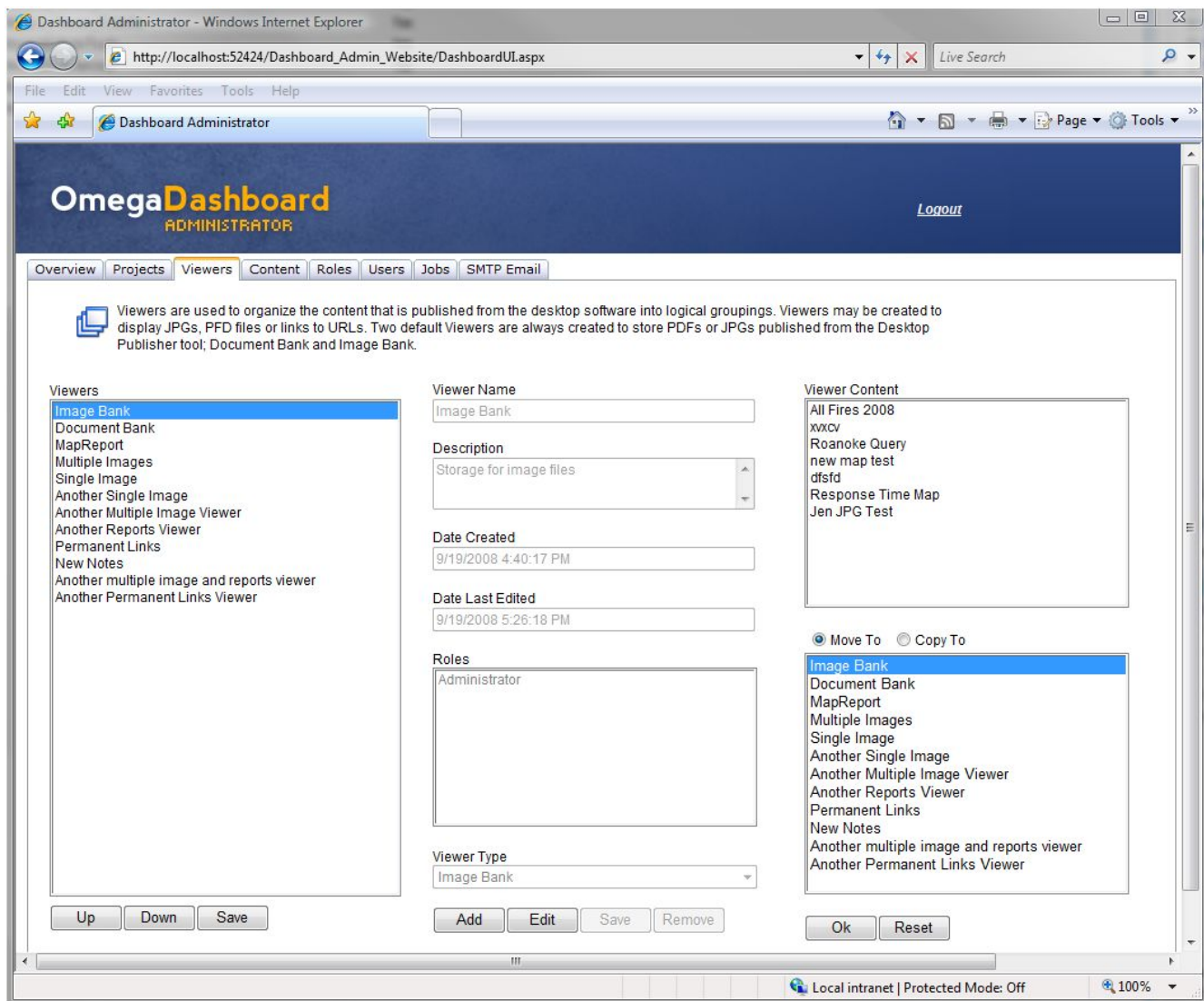
When a project is selected in the Registered Projects list, detailed information about the project is updated on the Project Tab. The information provided includes the project alias, the description, the date the project was registered, the last time project information was modified, and the machine name and path to the ArcMap project on the machine that is publishing the content. The Project Content list is also updated, and provides a quick overview of the content that has been posted to the server from the selected project.

Unregister Button

Before an ArcMap project can be unregistered, all content published from the project must first be detached. Detaching content from the project can be accomplished by deleting the content using the Dashboard Administrator Content tab. When all content has been removed, the best practise is to unregister the project using the Omega Desktop Administrator. However the 'unregister' button on the Project Tab has been provided in the event that the administrator cannot access the machine that was originally publishing content.

Viewers Tab

Viewers are the containers that are created to store and organize content. When a Viewer is selected from the Viewers list on the left side of the window, detailed information associated with the selected Viewer is updated. This information is described in the following sections.

Attachment A**Viewer Information**

The Viewer tab displays detailed information about each Viewer that has been created. In addition, it is possible to create, edit or remove Viewers from the application. Depending on the Dashboard application, the list of Viewers created may grow very long. The 'Up', 'Down' and 'Save' buttons below the Viewer list are available to provide a way to order the Viewers for manageability.

When a Viewer is selected from the Viewer list on the left side of the page, the information associated with that Viewer is updated. The name, description, date created and edited, roles, Viewer type and the content contained within the Viewer are then available. Once a Viewer has been selected, information pertaining to that Viewer may be updated using the Edit button; such as the name, description, and roles that are able to access that Viewer from the Dashboard Viewer web site. The Viewer Type may not be changed once the Viewer is created as the type of content that has already been published to the Viewer is very specific to the type.

The 'Add' or 'Remove' buttons are also available to create or delete Viewers. To create a new Viewer, a type must be selected, and at least one Role should be assigned. The Role determines who will be able to view the content from the Dashboard Viewer web site, while the Viewer type determines the type of information that can be published to the Viewer. To delete a Viewer, all content that was published to that Viewer must either be removed or copied to another Viewer. Content can be copied to another Viewer as long as it shares the same 'type'.

Viewer Types

There are nine Viewer types that enable content to be posted and displayed in a number of different ways on the Dashboard. The source of this content may include results generated by the Omega Desktop software, any file that is stored in JPG or PDF format, or messages that are posted using the Dashboard Administrator. The Viewer types used to display this information are described below.

Image Bank

The Image Bank Viewer is provided with the Dashboard application and cannot be deleted. It is provided by default in order to store information that is posted in JPEG format to the server. When a user publishes content from the Dashboard Publisher tool on a client machine, the data is automatically posted to this Viewer.

Document Bank

The Document Bank Viewer is also provided with the Dashboard application and cannot be removed. This Viewer type is capable of storing information that is

Attachment A

provided in PDF format. When publishing information from the Dashboard Publisher tool on a client machine, the data is automatically posted to this Viewer.

RSS Notes

The RSS Notes/Messenger Viewer stores messages that have been published by an author of the Dashboard. These messages appear in a chronological order, whereby the most recent message appears at the top of the Viewer. The 'Update Now' button can be used to retrieve any messages that may have been posted after the Dashboard was opened in the browser.

The Single Image Viewer

The Single Image Viewer displays a single image that has been published to the Dashboard. Any image may be published to the dashboard as long as it is in JPG format. Typically, these images may be maps or graphs published by the Omega Desktop software or other image files stored on disk that require distribution.

The Multiple Image Viewer

The Multiple Image Viewer is similar to the Single Image Viewer in that it will display any image provided that is in JPG format. The difference in this Viewer is that multiple images may be accessed by scrolling through the list using the 'previous' and 'next' buttons.

The Report Viewer

The Report Viewer lists published Portable Documents (PDFs) within a table in the Viewer. A title and description for each document is listed in the table, along with a Last Edited date. By clicking on the report link icon, these documents can be opened in a new Internet Explorer window or tab depending on your Internet Explorer settings.

The Temporary Links Viewer

The Temporary Links Viewer provides the ability for anyone logged into the Dashboard Viewer web site to add their own personalized web links. If the Viewer is removed from the Dashboard Viewer page however, the links will be removed as well.

The Permanent Links Viewer

The Permanent Links Viewer is similar to the Temporary Links Viewer in that it allows anyone logged into the Dashboard Viewer web site to add their own web links which can be accessed at any time. The difference in this Viewer is that if the Viewer panel is removed from the page, when it is added again, the previously created web links will remain.

The Multiple Image and Report Viewer

The Multiple Image and Report Viewer displays the results of a desktop analysis in the form of a map or graph with a linked report. The 'Enlarge Image' text can be clicked in order to display the map or graph in a new tab or window. The 'Review Report' text will open the PDF report in a new tab or window.

Content Tab

Content forms the building blocks of the Dashboard. Content may be published as images (JPG) or portable documents (PDF) from the Dashboard client machines. As it is posted to the server, each piece of content must be assigned to a Viewer as these form the containers that organize the published content.

When the Content Tab is opened, a list of available content can be viewed on the left side of the page. By default all of the content published is displayed, however, this information can be sorted by Machine, Project or Viewer. Selecting one of the categories will enable the administrator to narrow down the content within the list to a particular subset.

Attachment A
Editing Content

When an item of content is selected, the descriptive information regarding the content is updated as well. As content is published from the Dashboard client machines, the name, description, and template may be updated. Templates are available with reports, maps and graphs and refer to the associated file that is used to generate the content. It is important when changing the template that the source data be considered. The source data on which the new template is based, must be identical to the source data used to generate the original content otherwise when the content is updated it will fail.

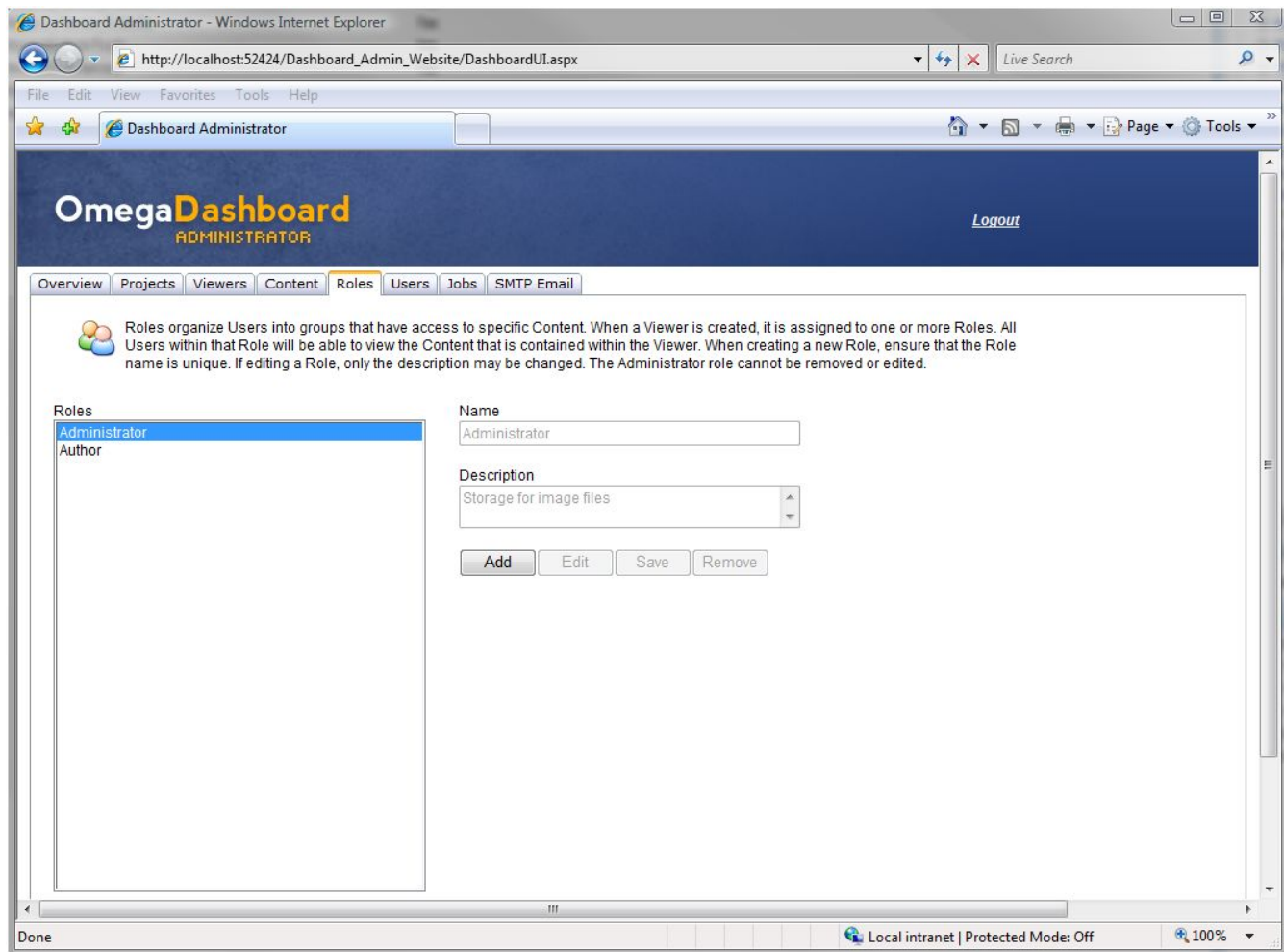
Automated Content

When content is posted from the Dashboard Wizard on the client machines there is the option to post the content as 'static' or 'automated'. Content posted from the Dashboard Publisher does not have this option; it is always static. If content is posted as 'automated', it can be selected on the Jobs Tab to form a job that can then be run from Windows Task Scheduler on the client machine. It is possible to change content from 'static' to 'automated' if it was posted from one of the routines that uses the Dashboard Wizard. In addition, the date query may be updated based on a previous date query.

Roles Tab

Roles are used to organize Users into groups so that the content they can view from the Dashboard Viewer web site is isolated to the Roles to which they belong. For example if a new User account is created, and they are assigned to the 'Narcotics Division' role, that means that the User will be able to see all of the Viewers that are also assigned to the 'Narcotics Division' Role. This allows the Administrator of the Dashboard to provide content to users that is appropriate to their specific discipline.

The Roles tab provides a means to add, edit or remove roles from the Dashboard application. If a role is to be removed however, all users assigned to that role must be removed prior to removing the role. Once a role is created, the name of the role cannot be changed. The role must be removed completely, and then added with the new name required.

Attachment A**Users Tab**

Users are defined as those individuals that will be accessing the Dashboard information posted to the server through a web browser. A user account must be created for each individual as the data that is posted to the Dashboard is personalized. The personalization of the data means that if two individuals log into the Dashboard using the same user account, when one individual makes a change to their Dashboard, the second individual will see these changes take effect.

The Users Tab lists all of the Users currently able to access the Dashboard application from a web browser. There are two users that are created with the application, and these cannot be deleted. The 'admin' account is created for the administrator of the Dashboard so they can log into the Administrator web site and organize the content. The 'Author1' account is created for anyone who might be posting messages to the Dashboard. The individual who holds this account may log into the 'authoring' page of the Dashboard Administrator web site, but does not have access to all of the other administrative web pages.

Users may be added, edited or removed from accessing the Dashboard Viewer application. When a new User is added, they should be assigned to at least one Role, which will allow them to View data that is posted to the Dashboard. Each new user must have a unique email address, and a password and security question. If the individual forgets their password, it is the security question that will be used to validate their identity.

Attachment A

Dashboard Administrator - Windows Internet Explorer

http://localhost:52424/Dashboard_Admin_Website/DashboardUI.aspx

File Edit View Favorites Tools Help

Dashboard Administrator

Logout

Overview Projects Viewers Content Roles **Users** Jobs SMTP Email

User accounts must be created in order to access the Dashboard Content that is published from the Omega Desktop software. Each User must be assigned to at least one Role. It is the Role that determines the Content can be viewed by the User.

Users

- admin
- Author1
- Joe

Name

admin

Email

jennifer@theomegagroup.com

Password Change Security

Confirm Password

Security Question

who am i

Security Answer

Roles

Administrator

Account Date

5/10/2007 2:19:34 PM

Last Login Date

12/23/2008 8:57:54 AM

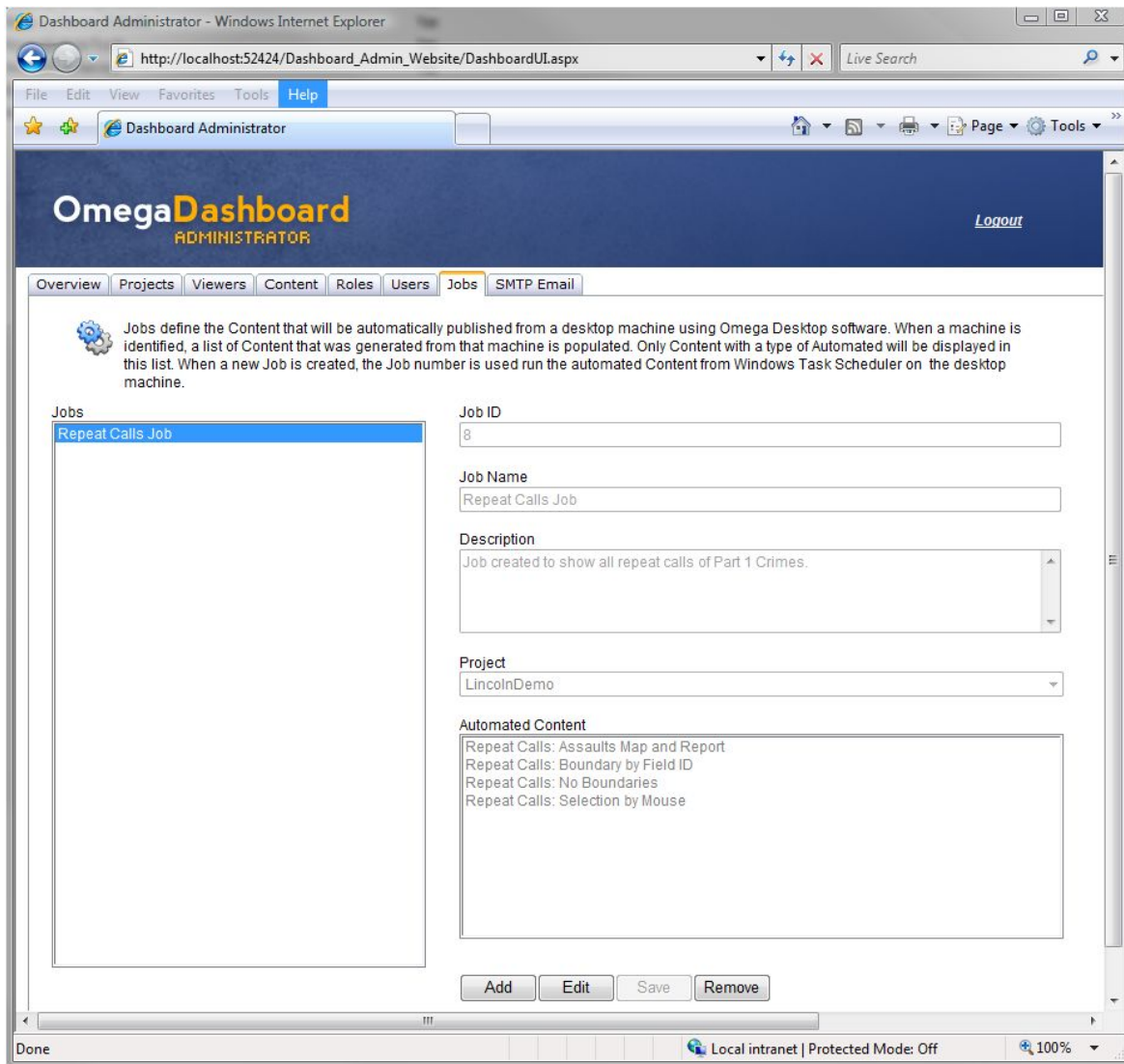
Add Edit Save Remove

Local intranet | Protected Mode: Off 100%

Jobs Tab

The Jobs tab is where automated content can be grouped in order to run it as a Scheduled Task in Windows Task Scheduler from the Dashboard client machine from which it was published. Only content that is posted from the same ArcMap project can be grouped into a single Job. When the Job is run, ArcMap is opened, and each of the content items that is selected for the Job is run in the order supplied.

When automating content that will be generated as maps, it is important to consider which content to group as a single job. When a Job is run, ArcMap is opened and each piece of content is run and added to the ArcMap project as a new layer. To avoid having layers piling up on top of one another, it is recommended to run each routine type together as one job. For instance, running several hotspot content maps together will only show one hotspot at a time, as previous layers are removed each time a new layer is created; this is a function of the Omega Desktop software.

Attachment A**Setting Up a Job**

Creating a new job involves adding a new Job Name, Job Description, and then selecting from a particular project all of the content that should be run from that Job. When the 'Save' button is clicked, a new automated Job Number will be created. It is this Job number that must be used when creating the Automated Task in Windows Task Scheduler.

To set up the Job, the administrator must go to the client machine from which the ArcMap project is running, and create a new Windows Task in the Scheduler. The task should point to the DashboardAuto.exe file in the \program files\omegagroup\desktop\bin folder, and the Job number should be referenced.

SMTP Server Tab

The SMTP Server tab is available in order to set up the SMTP server settings that will be used if an individual loses their user information. On the Dashboard Viewer and Administrator sites, the Forgot Password? hyperlink allows an individual to enter their email address in order to retrieve their login information. It is the SMTP server that will be used to email the individual their credentials. After updating this information, the Save button must be used in order to store the updates.

Attachment A

Dashboard Administrator - Windows Internet Explorer

http://localhost:52424/Dashboard_Admin_Website/DashboardUI.aspx

File Edit View Favorites Tools Help

Dashboard Administrator

Logout

Overview Projects Viewers Content Roles Users Jobs SMTP Email

SMTP configuration settings are required in order to make use of the Forgot and Change Password options. If the Dashboard Administrator has forgotten their username or password, the SMTP server sends this information via email to the User.

SMTP Settings

SMTP Server Name
sherlock

SMTP Port
25

SMTP From Email Address
jennifer@theomegagroup.com

Authentication

None

NTLM (Windows Authentication)

Basic (User Name and Password required)

Sender's Name

Sender's Password

Save Clear

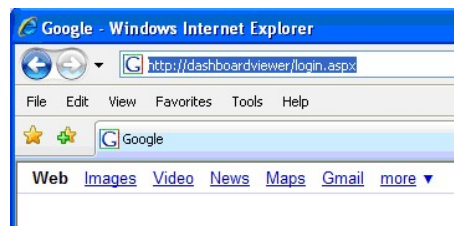
Done Local intranet | Protected Mode: Off 100%

The Dashboard Viewer**Introduction**

The Dashboard Viewer is a web site that is used to bring together maps, graphs, reports or other files so that the information can be distributed easily over the intranet. The data that is published may be created using Omega Desktop products such as CrimeView or FireView, however, other files may also be accessed as long as they have been published in JPG or PDF format.

To view data that has been published to the Dashboard, a user must have been granted permissions by the administrator of the application. Depending on these permissions, the user will be able to see different 'views' of the data. For example, an officer working within the fraud unit of a police department may only see maps and reports related to incidents of fraud, while a firefighter working in District 1 may have a view of all relevant incidents related to that particular district.

The Dashboard Viewer is available from a URL that is set up by the Dashboard Administrator personnel. Contact your administrator to be provided with this URL. Once the URL is identified, it is recommended that Internet Explorer 7 be used to view the web site. It is possible however to use IE6, however some of the features that are used with the Dashboard are not available in this version.



Attachment A**Elements of the Dashboard**

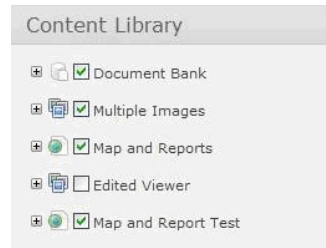
The layout of the Dashboard is divided into three parts. A panel on the left side of the Dashboard provides an area that is customized to the client's Dashboard application. An options strip allows the user to add or remove content, or hide or show the left panel. The remainder of the browser window is available for placing Viewer containers onto the screen. These elements of the Dashboard will be discussed in detail within the following sections.

The Content Library

The Content Library is located on the left side of the Dashboard window. This library lists all of the Viewer containers that may be shown to the user. Viewers are assigned to roles, and so if the user is a member of the same role assigned to that Viewer, the Viewer container will appear in the Content Library list.

A user may have a different list of Viewers available than other personnel within the department depending on the permissions that have been granted. Viewers are collections of data, and come in several varieties. These will be discussed in detail later on in this document.

There are several varieties of Viewers that have been created in order to provide different ways of viewing the information posted to the Dashboard. The Viewer types can be discerned by the different icons located to the left of the Viewer name. Hovering over these icons with the mouse will open a tooltip that displays the Viewer type.



A Viewer may or may not have data residing within it at the time the Dashboard is opened. If a Viewer has data within it, a checkbox will appear next to the Viewer name. If data has not yet been published to the Viewer, a checkbox will not be available.

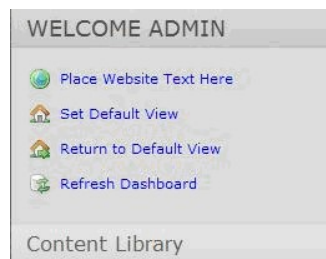
A user can always expand a Viewer within the Content Library by clicking on the plus sign to the left of the Viewer name. Expanding the Viewer will reveal a description about the content contained within it. If the administrator of the Dashboard has not included a description, the text 'No Description' will be supplied.



If a checkbox is located next to the Viewer name this indicates that data is available within the Viewer. After expanding the plus sign to reveal the description, the description itself can be expanded to reveal the content within the Viewer. Content may include reports, maps, graphs or pictures that are published to the Dashboard.

Dashboard Options

Above the Content Library is a section that is available to customize the Dashboard. The first item in this section is a link to the client's website. This link may or may not be displayed depending on whether the Administrator configured the link to be available. The next two features are available in order to create a Default View that is available to each Dashboard user. When a user clicks the 'Set Default View' text, all Viewer panels that are currently available on the Dashboard screen are saved. If the user wishes to return to this particular view of the information, it has been saved. To return to the Default View, the 'Return to Default View' option can be clicked. Finally, the 'Refresh Dashboard' option is available so that the user can update the Dashboard with any information that has been published to the server after the Dashboard was opened.

**Showing and Hiding Content**

Adding and removing all Viewers from the Dashboard can be accomplished using the options available at the top of the Dashboard window. 'Add All Content' adds all of the Viewers listed in the Content Library, while 'Remove All Content' clears the Dashboard of all Viewers. The Hide/Show Content Library can be clicked in order to temporarily hide the Content Library panel to provide more screen real estate.

The Dashboard Window

The Dashboard Window is the screen real estate to the right of the Content Library panel. Viewers can be added to the screen horizontally or vertically, and this option is configured by the Dashboard Administrator. This region appears as a single area for placing Viewers, however, it is actually divided into three columns. Viewers that are placed within this region can be moved between columns or ordered within each column.

The Viewer

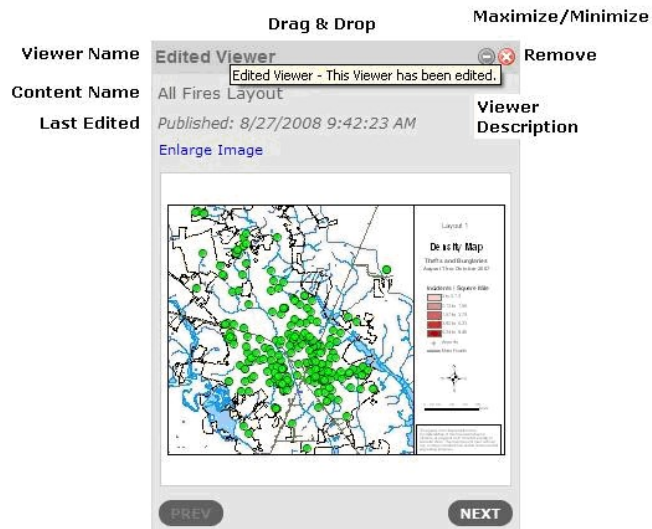
The Viewer is the building block of the Dashboard. Viewers are designed to present information in a variety of formats depending on the type of data on which

Attachment A

they are based. Although there are different types of Viewers available, there are certain elements that are common to all Viewers; these elements are outlined below:

The Viewer Title Bar

The Viewer title bar is common to all Viewers and is located at the top of each Viewer window. The title bar has several elements all of which are explained below.



Viewer Name: The Viewer name is displayed as the first line in the title bar. The name is created by the administrator of the Dashboard application.

Viewer Description: The Viewer description is visible by hovering the mouse over the title bar. The description is set by the administrator of the Dashboard when the Viewer is created.

Drag and Drop: All Viewers are capable of being moved within the three columns of the Dashboard Window. Moving the Viewer is accomplished by clicking on the title bar, holding down the left mouse button, and then dragging the Viewer to the new location.

Minimize: The Viewer window can be collapsed by clicking on the 'minus sign' icon in the title bar of the Viewer.

Maximize: The Viewer window can be expanded by clicking on the 'plus sign' icon in the title bar of the Viewer. The 'plus sign' icon is only visible when the Viewer is collapsed.

Remove: The Viewer can be removed from the Dashboard window by clicking on the 'x' icon in the title bar of the Viewer. When a Viewer is removed, it is only temporary. The Viewer can be added again by clicking on the Viewer checkbox in the Content Library and clicking 'Add'.

Last Edited: All Viewers show a 'Published' date that indicates the last time the data was updated. In most cases the Last Edited date appears below the Viewer name in the title bar. This date reflects the last time the data showing within the Viewer window was updated. In cases where there are multiple links to data within the Viewer window, the Last Edited date is displayed for each data item.

Viewer Types

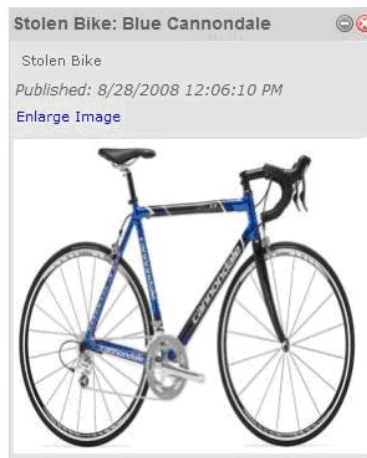
There are seven Viewer types that enable content to be posted and displayed in a number of different ways on the Dashboard. The source of this content may include results generated by the Omega Desktop software, any file that is stored in JPG or PDF format, or messages that are posted using the Dashboard Administrator. The Viewer types used to display this information are described below.

The Messenger

The Messenger Viewer lists messages that have been published by an author of the Dashboard. These messages appear in a chronological order, whereby the most recent message appears at the top of the Viewer. The 'Update Now' text can be used to retrieve any messages that may have been posted after the Dashboard was opened in the browser.

Attachment A**The Single Image Viewer**

The Single Image Viewer displays a single image that has been published to the Dashboard. Any image may be published to the dashboard as long as it is in JPG format. Typically, these images may be maps or graphs published by the Omega Desktop software or other image files stored on disk that require distribution.

**The Image Bank or Multiple Image Viewer**

The Image Bank and Multiple Image Viewer are similar to the Single Image Viewer in that it will display any image provided that is in JPG format. The difference in these Viewers is that multiple images may be accessed by scrolling through the list using the previous and next buttons.

The Image Bank Viewer is a default Viewer that is provided for all content that is posted to the server using the Omega Desktop Dashboard Publishing Tool. Content that is posted to this Viewer may be moved to a Single Image Viewer or another Multiple Image Viewer.



Attachment A**The Document Bank and Report Viewer**

The Document Bank and Report Viewer list published Portable Documents (PDFs) within a table inside the Viewer panel. The Document Bank is a Viewer that is provided by default to hold all PDF content posted using the 'Publisher Tool' within Omega Desktop. Only one Document Bank Viewer can exist, however the Report Viewer type can be created to hold other PDF material. In addition, PDF's that are posted to the Document Bank Viewer can be moved or copied to other Report Viewers.

For these Viewer types, a title and description for each document is listed in the table, along with a Last Edited date. By clicking on the 'open report' icon, these documents can be opened in a new Internet Explorer window or tab depending on the Internet Explorer settings.



Name	Description
 All Fires Report	No Description: Published: 8/27/2008 11:22:34 AM

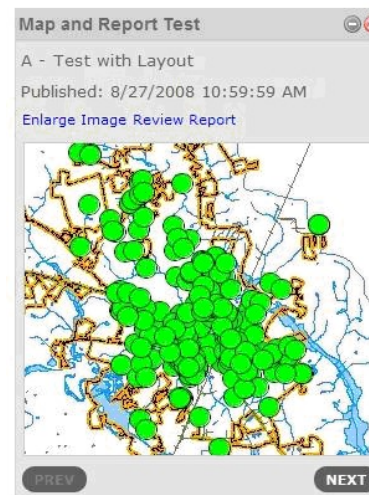
The Temporary and Permanent Links Viewers

The Temporary and Permanent Links Viewers are used to add links to other websites by identifying the web URL. The difference between these Viewers is that if a Temporary Links Viewer is removed from the Dashboard Screen, when it is reopened, the links are lost. The Permanent Links Viewer will retain these links if the Viewer is removed and then added back into the Dashboard.

These links are visible only to the person logged in using their specific account. When navigating with these links, the new website is opened in a new Internet Explorer window or tab depending on the IE settings.

**The Multiple Images with Reports Viewer**

The Multiple Images with Reports Viewer displays the results of a desktop analysis in the form of a map or graph with a linked report. The 'Enlarge Image' text can be clicked in order to display the map or graph in a new tab or window. The 'Review Report' text opens the PDF report in a new tab or window.



CrimeView Main Menu

The CrimeView main menu is the starting point for running crime analysis routines. To access the main menu select the Sherlock button on the CrimeView toolbar.



This button opens the [Queries](#) dialog that provides four routines for selecting incidents. The routines include; Attribute Query, Within A Boundary, Near An Address and Near A Feature.



This buttons opens the [Density Map](#) dialog that contains three routines; Density Map, Hot Spot Map and Repeat Calls.



This buttons opens a dialog that allows one to select one of the following routines: [Exception Reporting](#), [Spatial Trend](#) and [Crime Rate Generator](#).



This button opens the [Cyclical Reports](#) dialog that allows one to edit and run saved query and density map routines.



The button opens the [Threshold Alert](#) dialog.

Building An Application

Building a CrimeView application is a complex process that is unique for each client. Building the CrimeView application is typically a service provided by The Omega Group. This section highlights the major tasks when building the application.

[Retrieve Incident Data](#)

[Build Saved Queries](#)

[Build Crystal Reports](#)

[Set Default Fields](#)

[Create ArcMap Document](#)

[Create Map Templates](#)

Retrieve Incident Data

One of the first tasks in building a CrimeView project is retrieving the incident data. The incident data is used for analysis and provides the source data to create maps and reports.

The *Omega Import Wizard* provides a means to import datasets from Database Management Systems (DBMS) or ASCII text files. Once retrieved, the datasets are geocoded so that they may be used with OmegaGIS.

An Import Profile (*.oiw) is a file used by the Omega Import Wizard to outline the steps needed to retrieve and process the datasets. The Import Profile provides a processing template that records how to extract the dataset from the DBMS, which OmegaGIS fields to create, the geocoding steps involved and the final destination for the resulting feature class. Refer to the Omega Import Wizard documentation for further information.

Build Saved Queries

Attribute queries using SQL syntax to select features from incident datasets can often become lengthy and complex. [Saved Queries](#) hide the SQL syntax from the user while providing a more intuitive name or description for each query. Saved queries are created and edited with the [Saved Queries Editor](#) in ArcCatalog and are stored in the Omega_Query.MDB database.

Build Crystal Reports

CrimeView employs [Crystal Reports](#) for reporting functionality. Using the [OmegaGIS Metadata Editor](#), reports are registered to layers.

Set Default Fields

Attachment A

Using the [OmegaGIS Metadata Editor](#), set the default fields for the layers used by the CrimeView application. The default fields include:

- OmegaGIS Fields (date, day of week, time, response time).
- Incident Type for [graphs](#).
- Default field for list boxes in dialogs.

Create ArcMap Document

An ArcMap document containing incident datasets and other geography such as street centerlines provides the backdrop for performing geographic crime analysis. Every ArcMap document that uses OmegaGIS has an associated [project workspace](#) where the results of the routines and preferences are stored.

When creating the ArcMap document, the points outlined below should be followed:

- ***All layers must have a unique name.***

Layer names in the table of contents are used by OmegaGIS routines for identification. If layers share the same name, the first layer in the stack is always used by OmegaGIS. If the name of the layer changes, Cyclical Reports or Threshold Alerts created with that layer, will no longer be able to recognize the source data, and an error will result. Consequently, it is important that all the layers are assigned a unique name in the table of contents, and retain their original names.

- ***Data Frames must have a unique name.***

The name of the data frame is used with OmegaGIS routines. Consequently, the data frame names must be unique and should not change.

- ***Use a projected coordinate system***

All layers and data frames should have a projected coordinate system (as opposed to a geographic coordinate system). This is not a requirement but it is recommended as a projected coordinate system will result in more accurate results.

- ***Performance checklist***

The documentation contains a performance checklist that has recommendations for setting up an ArcMap document which should be followed.

Create Map Templates

[Map templates](#) are used to define how the map elements in the layout will appear. Map elements include a title, agency logo, legend, north arrow and scale bar. Map templates can be used with both [Cyclical Reports](#) and [Threshold Alerts](#).

Query Layer

A Query Layer is point layer in the active data frame that can be used in OmegaGIS routines. An attribute and/or spatial query is used to select the features in the query layer.

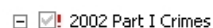
The Query Layer is set on the **What?** tab. When the Query Layer is selected, the [Saved Queries tree](#) (or columns) is updated with the saved query group(s) that are registered to the layer. The list of [additional query layers](#) is also updated.



Query Layer Criteria

When the OmegaGIS routine dialog opens, the list of query layers is populated. For a layer to be included in the list, the layer must meet the following criteria:

- The layer must be in the active data frame.
- The layer must be valid; the data source of the layer is not missing. When the data source is missing the layer will have a red exclamation mark in the table of contents.

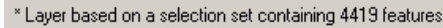


- The layer must have the geometry type of point. Layers with the geometry type of multi-point, such as layers created by the [Repeat Calls/Student Concentrations](#) routine, are not supported as query layers.
- The layer must have the data source of shapefile, Personal Geodatabase, File Geodatabase or ArcSDE.
- The layer must not be a selection layer. A selection layer is created from a subset of feature selected from another layer in the active data frame. A selection layer may also be created by [Query](#) routines when the query results option is "Show only selection (as new layer"; this option is set in the OmegaGIS Setup dialog.

To determine if a layer is a selection layer, use the Layer Properties dialog; in the table of contents right-click the layer and select

Attachment A

Properties; then make the Definition Query tab active. There will be a label at the bottom of the dialog if the layer is a selection layer, similar to the following image:



* Layer based on a selection set containing 4419 features

- The layer has the appropriate registered layer type. Layers may be registered in OmegaGIS as 'Incident', 'Person', 'Student' or 'Other' with the [OmegaGIS Metadata Editor](#). There is an option in the [OmegaGIS Setup](#) dialog that will only populate the list of query layers with layers that have a certain registered type. With this option selected, the list of layers is limited to only those layers of interest for querying.
- The layer has not been created from an OmegaGIS routine. An example of layer created from an OmegaGIS routine would be a [Composite Layer](#). There is an option in the [OmegaGIS Setup](#) dialog that controls whether to exclude layers created from OmegaGIS routines in the list of query and boundary layers.

Tip

- If a layer is added to the active data frame while the routine dialog is opened, the list of query layers will not be updated. To update the list of query layers, close the dialog and then open again.

Additional Query Layers

All [Query](#) and [Density Map](#) routines have the option to query multiple additional layers at a time. This functionality has been built into OmegaGIS to allow users to break apart point data into different layers (feature classes) to improve performance and still have the ability to query all of the features.

Omega recommends shapefiles contain 100,000 or fewer records while personal geodatabase be limited to 250,000 records. Typically, feature classes are divided by a date range or geographic area to accommodate these restrictions.

This section is divided into the following categories:

[Layer Criteria](#)

[Use of Additional Query Layers](#)

[AddQueryLayers.MDB](#)

[Composite Layer](#)

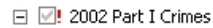
[Considerations when using additional query layers](#)

Layer Criteria

In order for a layer to appear in the list of additional query layers, the layer must meet the following criteria:

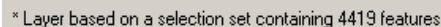
Attachment A

- The layer must be in the active data frame.
- The layer must be valid; the data source of the layer is not missing. When the data source is missing the layer will have a red exclamation mark in the table of contents.



- The layer must have the geometry type of point.
- The layer must not have the same feature class as the [Query Layer](#). In other words, the layer must have the same data source as the Query Layer.
- The layer must not be a selection layer. A selection layer is created from a subset of features selected from another layer in the active data frame. A selection layer may also be created by [Query](#) routines when the query results option is "Show only selection (as new layer)"; this option is set in the [OmegaGIS Setup](#) dialog.

To determine if a layer is a selection layer, use the Layer Properties dialog; in the table of contents right-click the layer and select Properties; then make the Definition Query tab active. There will be a label at the bottom of the dialog if the layer is a selection layer, similar to the following image:

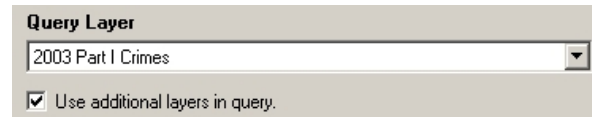


- The layer must have the same saved query group(s) of the [Query Layer](#). A saved query group contains attribute queries that are used to select incidents. The saved query groups are registered to a layer using the [OmegaGIS Metadata Editor](#).
- The layer must have the same spatial reference as the [Query Layer](#); it is not required that the layer share the same X-Y domain as the Query Layer because the X-Y domain is created dynamically. Consequently, layers that are based on a different geographic regions (i.e. City or Police Beat) can be used.
- The layer cannot have been created from an OmegaGIS routine. The "Exclude layers created from OmegaGIS routines..." option in the [OmegaGIS Setup](#) dialog controls this check.
- The layer must have at least the same fields as the [Query Layer](#) and the fields have the same type.

Use the utility in [OmegaGIS Setup](#) to determine why layers are not included in the list of additional query layers.

Attachment A**Use of Additional Query Layers**

To enable the use of additional query layers, on the **What?** tab first select the [Query Layer](#) and then check the "Use additional layers in query" checkbox.



When the checkbox is selected, all of the layers in the active data frame that meet the criteria listed above are added to the list. Check the layers to be included in the routine. When the Query Layer is changed, the list of additional query layers will be cleared and then updated with a list of layers that meet the criteria using the new Query Layer; the selection of the layers to use will be lost.



When there are no additional query layers, a message appears in the list.



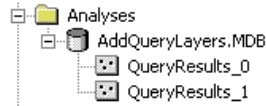
At the completion of the [Query](#) and [Density](#) routines, the [Query Layer](#) and those layers selected as additional query layers will have the following done:

- The layers will not be visible.
- The selected features in the layers will be cleared.
- The OmegaGIS [definition expression](#) on the layers will be removed.

AddQueryLayers.MDB

When additional query layers are used, the features selected by the attribute query and/or spatial query, are exported into the same feature class in a personal Geodatabase.

- The Geodatabase is named AddQueryLayers.MDB and is located in the "\Analyses" folder in the project workspace.

Attachment A

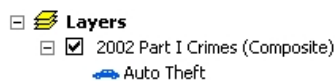
- The AddQueryLayers.MDB is created dynamically by the OmegaGIS [Query](#) and [Density Map](#) routines. If the Geodatabase is not present it will be created when the routine is run.
- An option exists in the [OmegaGIS Setup](#) dialog that creates a field in the new feature class called "OmegaGIS_Source". When this option is selected, this field is populated with the name of the source layer for each record.
- When the feature class in the AddQueryLayers.MDB is no longer in the data frame, it is deleted by the [OmegaGIS Project Exit](#).

Tip:

- To permanently persist the feature class created from a Query routine, use ArcCatalog to copy the feature class to another Geodatabase.

Composite Layer

When additional query layers are used with [Query](#) routines, the incidents selected by the attribute query and/spatial query are exported to a new feature class. This feature class is then added to the active data frame as layer. This layer is referred to as a "Composite Layer" in OmegaGIS since it has been generated from multiple layers.



- The name of the new layer is copied from the Query Layer with "(Composite)" added to the end of the name.
- The legend of the Query Layer is copied to the new layer, provided that the legend uses one of the following renderers:
 - A Unique Value renderer. The renderer can only use one value field.
 - A the Single Symbol renderer.

If the Query Layer legend does not meet the conditions outlined above, a default Single Symbol renderer is used.

- By default, a Query Layer can have only one "Composite Layer"; this can be changed in the [OmegaGIS Setup](#) dialog.

Attachment A**Considerations when using additional query layers**

The following considerations should be taken into account when using additional query layers:

- When running a [Query](#) or [Density Map](#) routine, always use an attribute query and a spatial query when appropriate. The use of the query will limit the features selected which will assist in the performance of the routine.
- When layers are broken apart by date, ensure that incidents are not duplicated among the layers.

For example, an incident occurring in January 2002, is imported from the client database, geocoded and inserted into the "Incidents 2002" layer by the Omega Import Wizard. One year later in January 2003, the incident is updated in the client database and inserted into the "Incidents 2003" layer. When the "Incidents 2003" layer is used in conjunction with the "Incidents 2002" layer during a query, duplicate information from the layers leads to an incorrect incident count.

To prevent an incorrect count of the incidents, layers should be free of duplicate values. Eliminating the potential for duplicate incidents in the resulting data can be achieved by correctly setting the Output Steps in the Omega Import Wizard (refer to the Omega Import Wizard Documentation).

Saved Queries

Attribute queries using SQL syntax to select features from a dataset can often become lengthy and complex. Saved Queries hide the SQL syntax from the user while providing a more intuitive name or description to each query. Saved queries are created and edited with the [Omega Query Editor](#) in ArcCatalog and are stored in the Omega_Query.ODB database.

This section is divided into the following topics:

[Saved Query Group](#)

[Select Saved Queries](#)

[Support for Different Query Layer Formats](#)

[Editing the Query](#)

[Finding a Saved Query](#)

[Query Grouping](#)

[Unique Value Query](#)

[Query Viewer Information](#)

Saved Query Group

Attachment A

A saved query group is comprised of a collection of saved queries. One or more query groups may be registered to layers used in ArcMap. Registering the query groups ensures that the saved queries are available to the assigned layers during OmegaGIS routines. Registration is possible through the use of the [OmegaGIS MetaData Editor](#) in ArcCatalog.

To determine the saved query groups that are registered to a layer, use the [Omega tab](#) in ArcMap. When the layer is selected in the table of contents, the metadata for that layer is displayed at the bottom of the Omega tab. The Query Groups item lists all of the registered saved query groups available to the selected layer.



Selecting Saved Queries

Saved queries are available on the **What?** Tab of Omega Desktop Query, Density and Analysis dialogs within the Saved Queries Tree or Saved Queries Columns structure. The tree or column structure is available based on a Setup setting.

Tree View

If the 'Tree' structure is selected in Setup, then a hierarchical structure of folders and checkboxes identify the queries associated with each Saved Query Group.



When the saved queries are loaded into the tree view, those saved queries that have invalid SQL query syntax or lack the query syntax for the format are loaded in the tree but are disabled.

Column View

In a 'Column' structure, the first two columns contain the children of level 1 saved queries, while all remaining saved queries and Saved Query Groups are presented within a 'Tree' structure within the third column.

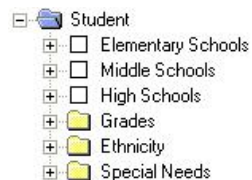
Attachment A

When the columns are populated with saved queries, those saved queries that have invalid SQL query syntax or lack the query syntax for the format are not populated in the list (in the tree view, the saved queries are disabled).

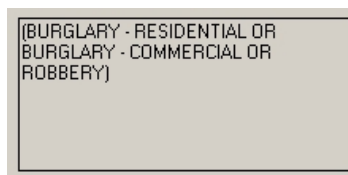
The [Omega Query Editor](#) is used to identify those saved queries that are to be displayed in the columns. This is done by selecting a level 1 saved query for each column; the level 2 children of those saved queries are displayed in the column. The name of the level 1 saved query is displayed at the top of the column. If the selected level 1 saved query has level 3 children, then these children saved queries are not displayed and there is a warning.

Selecting Saved Queries in Tree

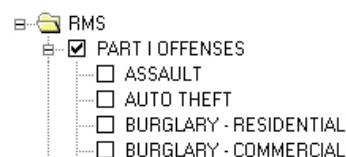
The content of the Saved Queries Tree (or columns) is made available once a [query layer](#) is selected during the routine. Displayed within the tree or columns, are all of the queries for each saved query group registered to the selected layer.



To select a saved query, select the check box in front of the name of the saved query. The selected queries are combined into a query string and shown to the right of the Saved Queries Tree.

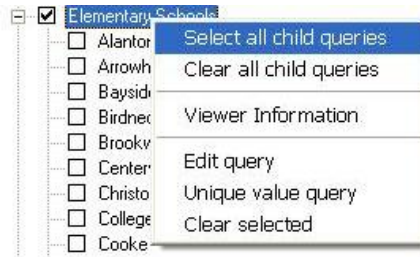


A parent saved query is identified in the query tree with a checkbox icon. The distinguishing factor between a parent saved query and a simple saved query is the list of saved queries that appear below the parent query. These saved queries are also identified by checkboxes. Selecting the parent saved query does not select or use all of the saved queries below it, but rather uses its own attribute query.



Attachment A

To select all saved queries under a parent saved query or category, right-click the item, and from the popup menu select "Select all child queries".



Select Saved Queries in Column

To select saved queries in the columns, simply select the saved query by clicking the mouse. Multiple saved queries can be selected by holding down the left mouse and while selecting all of the saved queries.

Another way to select multiple saved queries is to hold down the CTRL key while selecting the saved queries with the mouse.

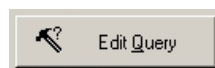
Support For Different Query Layer Formats

Currently, layers used by OmegaGIS can be stored in one of four different formats: an ESRI Shapefile, a personal Geodatabase (MDB) feature class, File Geodatabase or an ArcSDE feature class. Each of these formats requires a different SQL syntax. The benefit of using saved queries on a layer is that the appropriate SQL syntax is automatically applied, regardless of the format.

The [Omega Query Editor](#), available in ArcCatalog, can be used to build saved queries. In order for the saved queries to be available to all four layer formats, it must be built using the appropriate syntax for each of the data source types.

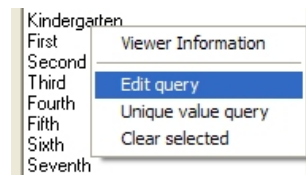
Editing the query

To manually edit the SQL syntax of a saved query, first select the query then click the Edit Query button. This button is only available when in Tree view.



Attachment A

To edit the query manually in Column View, right click within any of the columns and from the pop-up menu select Edit query.



The Edit Query dialog allows one to manually edit the SQL syntax. The dialog provides similar functionality as ArcMap's Select By Attribute dialog.

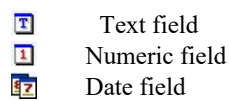
Query Layer Information

The header of the dialog provides the name of the query layer, the data source of the query layer and whether or not text queries are case sensitive.

Field List

The list on the left contains the names of all of the fields in the Query Layer. When this list is first loaded, the fields are in the order found in the feature class; clicking the field header will sort the fields.

The fields are given an icon based on the field type.



Note: all other field types are excluded from this list.

Unique Values

When a field is selected in the list, a sample of the unique values for that field is populated in the list on the right and the complete list button is enabled. The sample size for the unique values and the number of unique values to display in the list are controlled by the parameters set on the Advanced tab on the General view in Setup.

Complete List

When the list of unique values is first populated, only a sample of the feature class is used to determine the unique values. This sample size is controlled by Setup and the default value is set to 1,000. With this setting, only the first 1,000 records in the query layer are used to determine the unique values.

Attachment A

To populate the list of unique values using all of the records in the query layer, click the Complete List button. This processing may take a long time to complete and its use should be limited.

Restore

The Restore button clears the current attribute query and restores the original query from when the dialog was first opened.

Verify Query

The attribute query is tested when the Verify button is selected or when the OK button is selected.

- There is a warning reported if no records are selected. This message is only issued when the Verify button is selected. The message is not displayed when the OK button is selected as no records selected is still a valid query.
- The process of verifying the query does not alter what is selected in the query layer.
- The attribute query respects the definition expression and the selection layer features.
- The Omega definition expression is not removed when testing the query. The Omega definition expression may be removed while the running the routine; this may be the cause as to why no features are selected when the Verify button is selected.

Load and Save

There is the ability to save the attribute query to an .EXP unicode text file. This file can be used with ArcMap's Select by Attribute dialog. There is an issue bringing the attribute query into ArcMap, a symbol is added to the beginning of the attribute query that must be removed manually.

Build Query

To add either a unique value or field name to the attribute query, double click the item in the list. When there is text selected in the attribute query text box, that text is replaced. When there is no text selected and the cursor is located in the text box, the new text is placed at the cursor location; otherwise the new text is added to the end of the attribute query.

Close Dialog

To close the dialog and use the attribute query click the OK button. When the OK button is selected there is a check to ensure that the newly constructed attribute query is valid. An attribute query that does not select any features is considered a valid query.

When the attribute query is manually edited, the query is enclosed with brackets. This is to prevent problems with the order of operations when the attribute query is used with date queries. The brackets are not added if the manual edit created no text.

Attachment A

Furthering this, there is no change in the syntax based on the format of the query layer when the attribute query is manually edited. This could result in issues when using additional query layers and these layers are stored in different formats.

Finding a Saved Query

To find a saved query in the Saved Queries tree, type the phrase to be found and click the button with the binoculars icon. When there is a selected node in the tree, the search starts at the saved query below the selected node. When there is no selected saved query node, the first node is the start point for the search.



If the phrase is found, the saved query node is selected and the font bolded. The bold is removed when the Find button is used again, another node is selected or the pop-menu is displayed.

The search for the phrase is not case sensitive and the use of wildcards is not supported.

Query Groupings

Query groupings are used in the construction of the SQL query when joining multiple saved queries. Those saved queries that have the same query grouping are joined together with the "OR" connector while different query groupings are joined with the "AND" connector. As a general rule, query groupings are based on different fields, since a single record's field value can never equal two different values at the same time.

At previous releases, Query Groups only supported two query groupings; primary and secondary. At the version 4.0 of Omega Desktop it is now possible to commit up to 50 query groupings and assign a customized color to each group in order to aid in identifying the different groups when they are displayed in the tree format.

Query groupings are distinguished by the font color. This color is set in the [Omega Query Editor](#).



Building Query

The saved query view automatically combines the selected saved queries. Outlined below are the steps involved in generating the attribute query.

Attachment A

- All saved queries are surrounded with single brackets.

Example: UCR = 123 becomes (UCR = 123)

- All saved queries that share the same query grouping are surround with single brackets and joined with the OR operator.

Example: ((UCR =123) OR (UCR =124))

- Different query groups are joined together with the AND operator.

Example: ((UCR =123) OR (UCR =124)) AND ((MO = 84))

- When there are more then one query grouping, all of the saved queries are surround by brackets; this is to ensure order of operations when combined with date/time query.

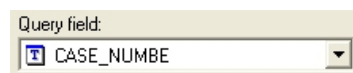
Example: (((UCR =123) OR (UCR =124)) AND ((MO = 84)))

Unique Value Query

The Unique Value Query dialog contains the functionality to automatically generate the attribute query to manually select features based on a field value. This functionality is helpful when a specific case number is known.

Query Field

At the top left of the dialog is a drop down list that contains the names of all of the text and numeric fields found in the query layer. When there are no text or numeric fields, the dialog is not opened and a warning message is displayed. The attribute query is based on this field.



When the dialog is first loaded, the query field is selected based on the following criteria:

- **Previous field used.**
- **The field identified as the "Default Field" in the query layers metadata. This information is set with the Omega Metadata Editor.**
- **The first field in the list.**

Attachment A

Manually enter value

To manually enter a field value, type the value into the text box and select the ">" button to move the value to the Values to query list. The use of wildcards are not supported. When the query layer has the data source of a Shapefile or File Geodatabase, the search is case sensitive.

Field Values

The Field Values list contains a list of unique values that is populated when the query field is changed. Both the number of unique values displayed in the list and the number of features in the query layer to search through to determine the unique values is controlled by parameters in Setup (located on the Advanced tab on the General view).

To select a unique value to query, select the item in the list and then click the ">" button. The selected item is added to the Values to query list and removed from the Field Values list.

Those unique values that contain a single quote do not appear in the list.

When the Unique Value Query dialog is used, the previously selected saved queries are cleared and only the unique value query is used. Up to 100 values can be queried.

Query Viewer Information

The Saved Query Viewer contains detailed trouble shooting information. When there is a warning loading the saved queries, a warning icon is displayed.



The warning information is available in the Query Viewer Information dialog. This dialog is accessed by either double clicking the warning icon or from the pop-up menu.

Warnings

The Warnings view contains all of the warnings that were encountered when loading the saved queries. Typical warnings include the registered saved query group is not found or saved queries exist containing invalid syntax for the format.

Query Groups

The Query Groups view list all of the registered query groups found in the query layers metadata.

Attachment A

- The order of the query groups is how the query groups are loaded when a Omega Query database is found.
- The icon provides information as to whether or not the query group has been loaded.
- When the query group is successfully loaded, the path to the Omega query database that was used is beside the name of the query group.
- When there are no registered query groups, there is a message on the list.

Database

The Database view contains all of the locations of the Omega query database that are searched for the query group information.

- The list is in search order. This search order is set on the Locations view in the Setup dialog.
- The icon identifies whether the status of the Omega query database.

Date and Time Ranges

Date and Time ranges are used by OmegaGIS routines to define spans of time from which to query features in a layer. Selecting features from a specific date and time range is possible for all layers that include OmegaGIS fields in the attribute table.

This selection is divided in the following topics:

[OmegaGIS Fields](#)

[Default OmegaGIS Fields](#)

[Selecting a Date Range](#)

[Selecting Day of Week](#)

[Organizing Date and Time Ranges](#)

[Clearing Date and Time Range](#)

[Available Date Range for Query Layer](#)

OmegaGIS Fields

Attachment A

Date and time attribute queries require fields that conform to a specific formatting standard. These fields are referred to as *OmegaGIS fields*, and can be created using the Omega Import Wizard. While importing data from a source database, the Import Wizard uses information from fields in the source dataset to generate the OmegaGIS fields.

The OmegaGIS fields currently supported include:

OmegaGIS Date: numeric field with the format of yyyyMMdd.

OmegaGIS Day of Week (DOW): numeric field with each day of the week having a different value. Sunday has a value of 0 and Monday has a value of 1. The value of -1 is assigned to incidents with invalid dates. The day of week field is created using the Date field.

OmegaGIS Time: text field with the hhmm format.

Although a standard data type and format are required for OmegaGIS fields, these fields do not require specific names. Unlike the date, time and day of week fields used with CrimeView and FireView for ArcView 3.x, multiple OmegaGIS date, time and day of week fields may be used within a single layer for analysis. Information about the OmegaGIS fields is stored in a layer's metadata and can be viewed using the OmegaGIS stylesheet in ArcCatalog. Layers do not require OmegaGIS fields to be used with OmegaGIS routines, however date and time queries will be unavailable if they are omitted.

Default OmegaGIS Fields

Given that OmegaGIS supports layers with multiple Date, Time and Day of Week fields, it is important to identify which fields will be used for querying features. The [OmegaGIS MetaData Editor](#) is available to set the fields that will be used as defaults during an analysis.

Steps in Determining the OmegaGIS Field

OmegaGIS routines follow several steps to determine which fields to use for date and time queries. Since it is possible to store multiple OmegaGIS date, time and day of week fields within the same layer, it is important to understand the method OmegaGIS uses to identify the fields used within a given routine. The following steps identify the mode of field selection:

- The layer's metadata is read to determine the default OmegaGIS fields.
- If no default OmegaGIS fields information is found in the metadata, the first date, day of week and time field found in the metadata is selected.
- If the layer has no metadata, such as when the layer has been created by legacy Avenue import scripts, the layer is searched for fields called "cvDate", "cvDOW" and "cvTime".

Attachment A

Tool Tips

A method exists for quickly determining which OmegaGIS fields will be used for date and time attribute queries. On the When? tab, available within OmegaGIS routines, hover over the Date, Time or Day of Week labels to view the tool tip that identifies the fields used to select features in the [Query Layer](#).

Date



Time



Day of Week

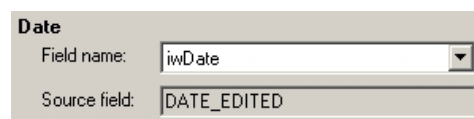


OmegaGIS Fields Dialog

To view or change the default fields temporarily for the current routine, click on the Options button of the When? tab to open the OmegaGIS Fields dialog. From this dialog, use the drop down list to alter the field.

Source field: Name of the field within the source feature class that has been identified in the metadata as an OmegaGIS field. If the layer lacks metadata information about the OmegaGIS fields, the source field text box will be blank.

Date range: The date range text box for the OmegaGIS Date field provides information on the start and end date found in the feature class; the date information is in yyyyymmdd format. The date range information is from the metadata of the feature class.



Selecting a Date Range

There are three ways to select a date range:

Previous Range

One option in selecting a date range employs the Previous duration selection. Select one of the duration types from the drop-down list: Hours, Days, Weeks, Months, or Years. The available numbers will change depending on the duration type that is selected. The ranges available include: 1 - 72 Hours; 1 - 90 Days; 1 - 52 Weeks; 1 - 24 Months; or 1 - 20 Years, respectively. When a duration is selected, the calendars at the top of the When? tab change to the range selected.

Attachment A

Previous 3 Weeks

The ranges identified by the Previous drop-down list describe completed blocks of time. If for instance, '1 Month' is selected from the list, and the current date is January 10th, the calendar dates on the dialog read December 1st through December 31st. The previous date range is identified as the last complete month, and the dates January 1st through January 10th are omitted. Similarly, selecting '1 week', updates the calendar dates with a range from December 29th through January 4th as that is the last complete week found. This concept carries on to days and hours.

The previous week date range uses a [setup](#) option to determine the day of the week to use as the start day. The default day for the start of the week is Sunday.

Predefined Date Range

In situations where a range of dates is required, up to and including the current day, the Predefined Date Range list is available. For example, selecting 'Month to Date' from the Predefined Date Range results in the selection of dates from January 1st to January 10th.

There are four standard predefined date ranges: Today, Week to Date, Month to Date, and Year to Date. Additional predefined date ranges can be created by manually selecting a date range and then clicking the Organize... button.

Predefined Date Range
MONTH TO DATE Organize...

When the predefined date range is selected, the calendars at the top of the When? tab change to the selected date range.

Manually Select Dates

Manually select a date range using the calendars at the top of the When? tab. Using the FROM Date calendar, select the month and year by clicking on the arrows. The calendar defaults to the current month. The date selected is shown on the upper right side of the calendar. Using the TO Date calendar, select the month and year by clicking on the arrows. Again the selected date is shown on the upper right side of the calendar.

FROM Date 11/10/2003

November		2003				
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

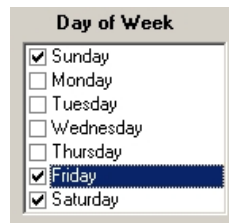
Attachment A

When the date range is selected, the Predefined Date Range reads as "OTHER". The calendar may have dates that are gray and cannot be selected. These are dates that fall outside of the layer's available [date range](#). In order to view a layer's available date range, the [OmegaGIS Setup](#) option 'Display available dates' on the Advanced Tab of the General Settings must be selected. If a layer is missing metadata information, the option 'Search the layer's feature class' for the date range may also be selected to determine the layer's available date range.

If the date range for a layer is not identified by the calendars on the When? tab, the settings in OmegaGIS Setup may not be selected. Alternatively, the routine may be using an additional query layer, in which case the layer's date range is unavailable.

Selecting Day of Week

Days of the week can be singled out for analysis by selecting each day from the Day of Week list on the When? tab. To select a day, check the checkbox next to the day of interest. To clear the days selected, right-click on the list, and select 'Clear Day of Week' from the popup menu. When all of the Day of Week values are cleared, the day of the week is not used in the attribute query.



If the OmegaGIS Day of Week field does not exist in the query layer, the Day of Week list is disabled.

Selecting a Time Range

A time range identifies the block of time used to select features from a layer during a routine. There are three ways to select a time range:

Previous Time Range

A previous time range based on hours is available from the Previous drop-down list. The number of available hours spans a time period of 1 to 72 hours. When a range is selected, both the FROM and TO calendars, as well as the FROM Time and TO Time controls are updated automatically.



Predefined Time Range

A time range can be selected using the predefined time range drop-down list on the When? tab. There are two standard predefined

Attachment A

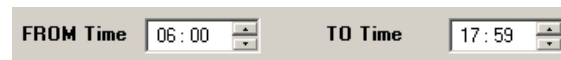
time ranges: Day (0600 to 1759) and Night (1800 to 0559). Additional predefined time ranges can be created by manually selecting a time range and clicking the Organize... button to open the Range Definitions dialog.



When a predefined time range is selected, the FROM Time and TO Time controls are updated.

Manually Select Times

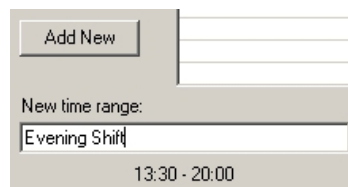
To set a time range manually, enter a time for the FROM Time and TO Time or use the arrow buttons to scroll to a time.



When a time range is entered manually, the predefined time range reads as "OTHER".

Organizing Date and Time Ranges

To manage the user created date and time ranges, click the appropriate Organize.. button. When saving a new date or time range, enter a title and click the Add New button.



The date and time ranges are stored in the *Settings.MDB* which is located in the OmegaGIS install directory; \OmegaGIS\Desktop\Databases. Predefined date and time ranges are available to any OmegaGIS application on the machine. The Organize button is disabled if the Settings.MDB cannot be found.

Clearing Date and Time Ranges

- Click the *Clear All* button to clear Date, Time and Day of Week selections.
- To clear only the date range, from the *Predefined Date Range* list select "ALL DATES".

Attachment A

- To clear only the time range, from the *Predefined Time Range* list select "ALL TIMES".

Available Date Range for Query Layer

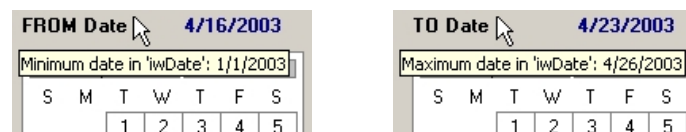
The FROM and TO calendars display the query layer's available date range based on whether the 'Display the available date' option is selected on the General Settings Advanced tab in [OmegaGIS Setup](#). When this option is selected, the Query Layer's metadata is read for the available date range. The metadata containing the date range is created if the layer is imported using the Omega Import Wizard.

If for any reason, the metadata is missing, the option 'Search query layer's feature class' on the Advanced tab of the General Settings in [OmegaGIS Setup](#) can be used to search the feature class for the available date range. It is important to note that using this option may result in a performance hit, especially if the layer contains a large number of records.

Provided that the settings mentioned previously are used, and the 'Use additional layers in query' checkbox on the What? tab is not selected, the calendars display the available date range in white, while those dates that are unavailable are grayed out. Unavailable dates cannot be selected.



The tool tip can be used to determine the available date range. Hold the mouse over the FROM Date label for the beginning of the date range, hold the mouse over the TO Date for the end of the date range.

**User Defined Area**

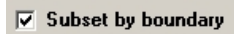
Attachment A

Many routines in OmegaGIS provide the option to create a user defined boundary to define a spatial filter. This tool is useful when there are no existing boundary layers that can be used to spatially query features.

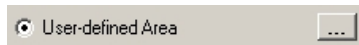
Create User Defined Area

To create a user defined area follow these steps:

- On the Where? tab select the "User-defined area" option. If the Where? tab is disabled, then on the How? tab check the Subset by Boundary checkbox.



- With the "User-defined area" option selected, click the ellipses button. This button will shrink the dialog and make the ArcMap "Polygon" tool active.



- To create the polygon in the active data frame, click each point along the polygon's boundary. Double-click the last point to complete the boundary.
- To expand the dialog, double click the red flashing icon in the upper right corner.

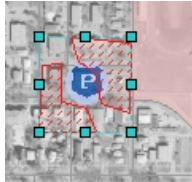
Requirements of User Defined Area

A user defined area is a graphic element. In order to run a routine using the graphic element as the spatial filter, the graphic element must satisfy the following requirements:

- Only one graphic element may be selected. An element is selected when it has handles around it's envelope.

Attachment A

- A graphic element cannot consist of a group of elements. Grouped elements are created by selecting multiple elements and selecting "Group" from the Drawing toolbar.



- The element must be a polygon.
- The element can have only one exterior ring. Complex polygons as seen below are not supported.



- The element cannot have an interior ring or donut.



Boundary Layer



Many OmegaGIS routines, including all [Density](#) routines, use a boundary layer to query features geographically.

Select Boundary Layer

Attachment A

The first step in selecting boundaries to be used in a spatial query is to choose the boundary layer from the list of layers on the **Where?** tab. The criteria used to populate the list of boundary layers is as follows:

- The layer must be in the **active data frame**.
- The layer must be **valid**; meaning the data source of the layer is not missing. When the data source is missing the layer has a red exclamation mark in the table of contents.

  2002 Part I Crimes

- The layer must have the geometry type of **polygon**.
- There is an option in the [OmegaGIS Setup](#) dialog that controls whether to exclude layers created by OmegaGIS routines in the list of boundary and query layers. An example of a layer created by an OmegaGIS routine might be a [density map](#). This layer can be excluded or included in the boundary layer list by toggling the setting in the OmegaGIS Setup dialog.

Selection Method

Once a boundary layer is selected, two **Selection Methods** are enabled, one of these options must be selected to continue.

By Field Value

The "By Field Value" selection method selects features in the boundary layer, such as a police beat or school district, based on an attribute value of the feature.

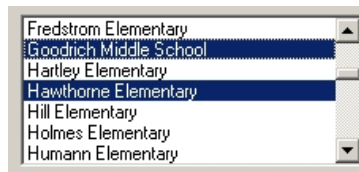
Field Name

From the Field Name drop-down listbox, select the field from the boundary layer that has values to be used to identify the features for the spatial query. The field should contain values that uniquely identify features in the boundary layer, such as the name of the school district. If an OmegaGIS default field is specified in the layer's metadata, this field is selected automatically. The OmegaGIS default field is set with the [OmegaGIS Metadata Editor](#).

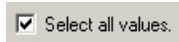


Field Values

From the list of Field Values, select the values that represent the feature to use in the boundary layer. To select more than one value, hold down the CTRL key. To un-select a value from the list, hold down the CTRL key and select the value.

Attachment A

To select all of the field values and use all of the features in the boundary layer, select the "Select all values" checkbox.



The Field Values list contains a unique list of values. In an effort to improve the performance of the OmegaGIS application, a predefined number of features in the boundary layer are used to determine the unique values. The number of features used to search for unique values is set in the [OmegaGIS Setup](#) dialog. For layers with a large number of features from which to search, select the Complete List button to sample each of the polygons found in the layer for unique values.

There is a limit to the number of unique values displayed in the Field Values list. This limit is set in the [OmegaGIS Setup](#) dialog. When the limit of unique values is reached, a warning is displayed to the left of the list. The maximum number of unique values that can be displayed in the Field Values list is 30,000. If this becomes an issue, use the By Pointing selection method.



By Pointing

The "By Pointing" selection method allows interactive selection of the boundary layer features used in the spatial query. With this option selected, click the ellipses button to shrink the dialog which makes the boundary layer visible and ensures that the boundary layer is the only selectable layer in the active data frame.



Click on the feature to select a polygon. To select multiple features, hold down the SHIFT key and click on the other features. Alternatively, select by dragging a box around the features. All of the features either touching or located within the box are selected.

When the selection is completed, double click the red flashing icon in the upper right corner of the dialog. The dialog will then expand to its normal size. The selectability of the layers will return to its state before the dialog was shrunk.

OmegaGIS.STYLE

Styles are collections of symbols and map elements that are used when setting the symbology of a layer. Styles are stored in files that have the .STYLE extension. ArcGIS provides several styles out of the box. OmegaGIS comes with it's own style file called OmegaGIS.STYLE.

When a routine is run, the OmegaGIS style is added to the ArcMap document; if it is not already there. The OmegaGIS style file is located in the "< Install Directory >\OmegaGroup\Desktop\Symbology" folder.

The OmegaGIS style file contains the colour ramps used by routines, such as the [Density Map](#) routine and point symbols.



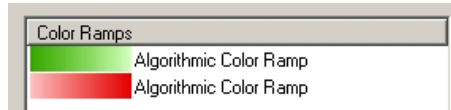
Modifying the OmegaGIS.STYLE

The color ramps used by the routines can be edited with the Style Manager in ArcMap. It is recommended that the OmegaGIS.STYLE file be backed up before any modifications are attempted. When editing the color ramps:

- The name of the color ramp cannot be altered.
- The category of the color ramp must be "OmegaGIS".
- The Exception_Report color ramp, used with the [Exception Reporting/Enrollment Comparison](#) routine and Exception Report Viewer/Enrollment Comparison Viewer, must be a 'Preset' color ramp. The figure below outlines which color is used with the class breaks of the layer.



- The DensityMap_* color ramps are used by [Density Map](#), [Crime Rate Generator/Demographic Analysis](#) and [Demographic Viewer](#) routines. These color ramps must be an 'Algorithmic' color ramp.
- The SpatialTrend_* color ramps, used by the [Spatial Trend](#) routine, are 'multi-part' which consist of two 'Algorithmic' color ramps.

Attachment A

Modifications made to the color ramps in the OmegaGIS style file will not be reflected in the routine dialogs, only with the resulting layers.

Omega Project Cleanup

The purpose of Omega Project Cleanup is to remove any temporary files that are created while using OmegaGIS software as well as clean up data sets that are generated by OmegaGIS but are not referenced by the ArcMap document. Project Cleanup is run automatically when the project is closed, but only if an OmegaGIS routine has been run. However, it may also be run manually from [OmegaGIS Setup](#).

The clean up procedures involved in Project Cleanup are outlined below.

[Remove Selection Layers](#)

[Remove OmegaGIS Feature Definitions](#)

[Remove Additional Query Layers](#)

[Remove Temporary Files](#)

[Clean Crime Rate Generator Database](#)

[Clear Demographic Analysis Database](#)

[Clean Demographic Viewer Database](#)

[Clean Exception Reporting/Enrollment Comparison Database](#)

[Clean Additional Query Layers Database](#)

[Clean Density Map Database](#)

[Clean Repeat Calls/Student Concentrations Database](#)

[Clean Residency Report Database](#)

[Clean Raster Layers](#)

[Clean Shapefiles](#)

[Compress the Selection Database](#)

Attachment A

Remove Selection Layers

Selection layers are the result of running the Query routines provided with OmegaGIS. A selection layer is not distinct, but is linked to the source data on which it is based. For instance, the data source of a new layer showing only those crimes classified as assaults, actually leads back to the Part 1 Crimes layer from which the assault crimes were drawn.

Selection layers are identified in the Table of Contents with the text (Selection) added to the layer name. A selection layer may also be identified by right-clicking on the Properties dialog and selecting the Definition Query tab. The text `*Layer based on a selection set&ldots;` identifies the layer as a selection.

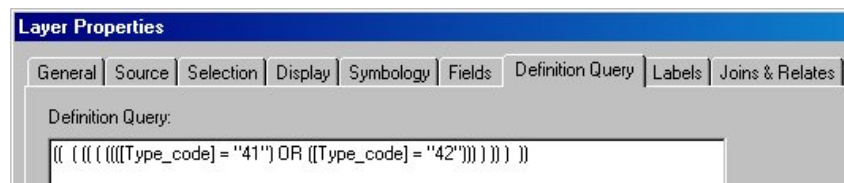
Depending on the setting in [OmegaGIS Setup](#) all Selection Layers are removed from the Table of Contents when Project Cleanup is run.



Remove OmegaGIS Feature Definitions

A feature definition is used in ArcMap to display features based on an attribute query. Only those features that satisfy the query are shown on the map. In OmegaGIS, this method is used as well when an OmegaGIS Query routine is run. If the appropriate setting is selected in OmegaGIS Setup, only those features selected by the query in the routine are displayed on the map.

An Omega Feature Definition is simply the query used to identify the output features of an OmegaGIS Query routine. An Omega Feature Definition can be recognized by right-clicking on the layer name in the Table of Contents, clicking Properties, and selecting `'Definition Query'`. An Omega Definition Query is delimited by a unique set of brackets `'(((((((((Omega Query Here))))))))'`.



During Project Cleanup, these feature definitions can be removed by setting an option in [OmegaGIS Setup](#).

Attachment A

Remove Additional Query Layers

[Composite layers](#) are created when more than one layer is combined during an OmegaGIS Query routine. The layer can be recognized in the Table of Contents by the term '(Composite)' that is added to the layer name.



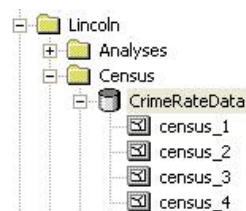
Composite layers may be removed from the project during a Project Cleanup by setting the appropriate option in [OmegaGIS Setup](#).

Remove Temporary Files

Temporary files are created when OmegaGIS routines and tools are run. These temporary files are used only while the project is open, and an OmegaGIS routine is in progress. As they tend to build up on disk, they are removed automatically when the project is closed or can be removed manually using [OmegaGIS Setup](#).

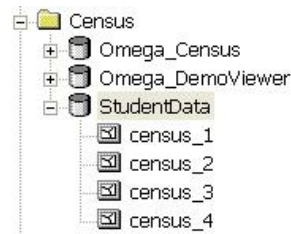
Clean Crime Rate Generator Database

The Crime Rate Generator Database (CrimeRateData.MDB) houses the data generated when a Crime Rate Generator routine is run in CrimeView. During a Project Cleanup, the feature classes in the Crime Rate Generator Database that are not referenced by layers in the table of contents are deleted.



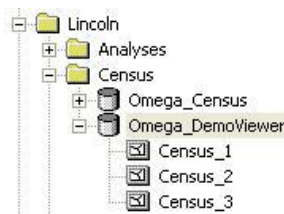
Clean Demographic Analysis Database

The Demographic Analysis database (StudentData.mdb) houses the data generated when a Demographic Analysis routine is run in School Planner. During a Project Cleanup, the feature classes in the Demographic Analysis database that are not referenced by layers in the table of contents are deleted.

Attachment A

Clean Demographic Viewer Database

The Demographic Viewer Database (Omega_DemoViewer.MDB) houses the data generated by the Demographic Viewer. During a Project Cleanup, the feature classes in the Demographic Viewer Database that are not referenced by layers in the table of contents are deleted.



Clean Exception Reporting/Enrollment Comparison Database

The [Exception Reporting/Enrollment Comparison](#) Database (ExceptionData.MDB) houses the feature classes and tables that are generated when the Exception Reporting/Enrollment Comparison Analysis is run. Each new Exception Reporting layer is based on a feature class holding the geometry of that layer and a table that includes the attributes necessary for reporting crime statistics.

The feature class is linked to the table based on metadata that is stored in both the feature class and the table. The metadata tag <theomegagroup>exceptionreporting\featureclass</theomegagroup> in the table identifies the feature class to which the table is linked. The metadata tag <theomegagroup>exceptionreporting\tablename</theomegagroup> in the feature class identifies the name of the feature class.

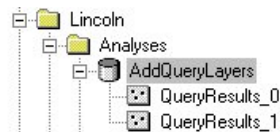
To clean up the Exception Reporting/Enrollment Comparison database, each table in the database is identified and the metadata tag containing the name of the linked feature class is read. If the feature class is not being used as source data for any of the layers in the table of contents, both the table and feature class in the database are deleted.



Attachment A

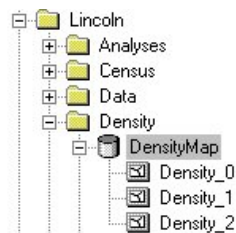
Clean Additional Query Layers Database

The [Additional Query Layers](#) database (AddQueryLayers.MDB) stores the source data of Composite layers. Composite layers are created when two or more layers are combined during a Query or Density routine. To clean up the database, feature classes within the database are compared with the source data of the layers in the table of contents. If the feature class within the database is not being used as the source data for any of the layers in the table of contents, the feature class within the database is removed.



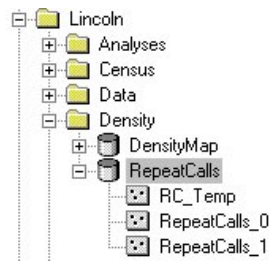
Clean Density Map Database

The [Density Map](#) Database (DensityMap.MDB) stores the source information used to display the results of the Density Map routine. Each time a new Density Map is created, a new feature class is created in the database on which the new layer is based. During a Project Cleanup, any feature class found in the database is removed, provided it is not referenced by any of the layers found in the table of contents.

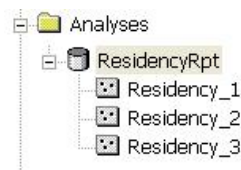


Clean Repeat Calls/Student Concentrations Database

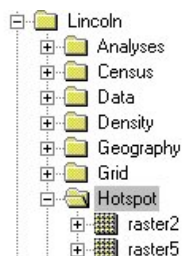
The [Repeat Calls/Student Concentrations](#) Database (RepeatCalls.MDB) houses the data generated when a Repeat Calls (Student Concentrations in School Planner) routine is run. During a Project Cleanup, the feature classes in the Repeat Calls (Student Concentrations) Database that are not referenced by layers in the table of contents are deleted.

Attachment A**Clean Residency Report Database**

The Residency Report Database (ResidencyRpt.MDB) houses the data generated when a Residency Report routine is run in School Planner. During a Project Cleanup, the feature classes in the Residency Report Database that are not referenced by layers in the table of contents are deleted.

**Clean Raster Layers**

Raster layers are created by both the [Hotspot](#) (Spatial Clustering in School Planner) and Spatial Trend Analysis <LINK> routines. The source data is stored in the \Hotspot folder, and it is this folder that is searched when a Project Cleanup is run. Raster data that is not used as the source data for any of the layers in the table of contents is removed.

**Clean Shapefiles**

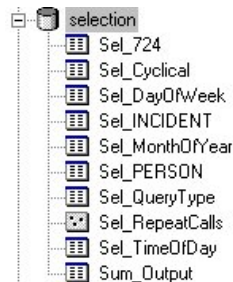
During certain routines temporary shapefiles are created in order to generate the final layers. These shapefiles are removed when the

Attachment A

project is closed as they are not necessary to the results of the routines.

Compress the Selection Database

The Selection Database (Selection.MDB) stores and formats temporary selection sets that are used to display reports and graphs. Since data is written to this database frequently, over time the database can become quite large due to the many additions and deletions of records. To keep the Selection Database size under control, it is automatically compressed when a Project Cleanup is run.



Persisting Routine Results

Most OmegaGIS routines create a new layer to display the results. These layers are typically removed from ArcMap's table of contents and deleted from disk with the [Project Cleanup](#). This help section outlines methods to persist these layers.

Selection Layers

A *selection layer* is created by Query routines when the query results option is "Show only selection as new layer"; this option is set in the [OmegaGIS Setup](#) dialog. A selection layer is created from a subset of features selected from another layer in the active data frame. No new feature class is created on disk as the same datasource is used as the source layer.

To determine if a layer is a selection layer, use the Layer Properties dialog; in the table of contents right-click the layer and select Properties; then make the Definition Query tab active. There is a label at the bottom of the dialog if the layer is a selection layer, similar to the following image:

* Layer based on a selection set containing 4419 features

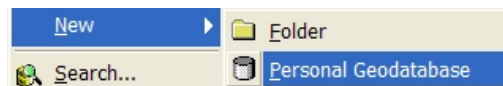
Selection layers may be removed with [Clear All](#). Once removed from the active data frame, selection layers are lost as the layer was only a subset of an existing layer. Furthering this, the datasource of the layer may change which alters the features available in the selection layer. For example, CrimeView applications typically have a Calls for Service (CAD) layer that is updated nightly by the Omega Import Wizard. The Omega Import Wizard has the ability to get all the records that have occurred in the last 5 days. During the import process, duplicate features in the datasource of the layer are removed based on a primary key, such as a call number.

Attachment A

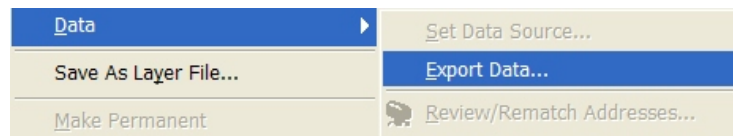
Once these duplicate features are removed, the newly imported features are appended. The selection layer may contain features that occurred 2 days ago which are removed and then replaced by the Omega Import Wizard. Although the call number remains the same, the ObjectID value is altered for the updated features and it is this ObjectID value that is used to determine the features in the selection layer. Consequently, there could be situations where after the import process, the selection layer will not contain the same features as when the selection layer was first created.

Follow these steps to permanently persist a selection layer so that it can be used at a future date:

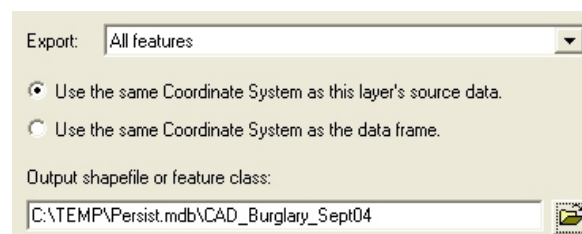
- If necessary, in ArcCatalog create a personal Geodatabase that is to be used to permanently store the selection layer. Right-click in the folder to create the personal Geodatabase and select New from the pop-up menu and then Personal Geodatabase.



- In ArcMap's table of contents, right click the selection layer and from the pop-up menu select Data and then Export Data.



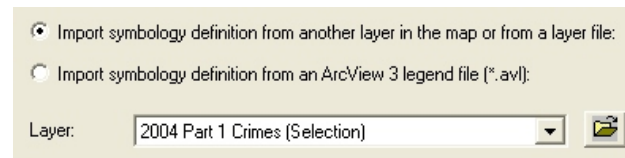
- From the Export Data dialog, select 'All Features' in the Export list and then click the browse button to navigate to a location to save the new feature class. A feature class is a term used to describe a layer that is store within a Geodatabase. It is recommended that the format of the new feature class be a Geodatabase.



- On the Export Data dialog, click the OK button to generate the new feature class. The newly exported feature class only contains the data and not the symbology information. To permanently persist the symbology, select 'Yes' when prompted to add the exported data to the map as a layer.

Attachment A

Open the Layer Properties dialog for the newly created layer and click the Import button on the Symbology tab. On the Import Symbology dialog, select the import symbology definition from another layer and then from the layer drop down list select the selection layer. Click the OK button to import the symbology.



To permanently persist the symbology create a layer file (.lyr). A layer file contains information on both the datasource and symbology of the layer. In the table of contents, right click the new layer and from the pop-up menu select Save as Layer File.

Save As Layer File...

The layer file can be added to an ArcMap document and the layer will contain the features from the selection layer and original symbology.

Result Layers

Result layers are those that are generated by an OmegaGIS routine, such as [Density Map](#). These layers are typically based on a newly generated feature class that are temporary stored in the [project workspace](#). When these layers are no longer referenced in ArcMap's table of contents then the source feature classes are deleted during the [Project Cleanup](#) that occurs when ArcMap is closed.

The process to permanently persist these result layers is similar to that as selection layers which is described in detail above. The source feature class must be copied to new personal geodatabase and a layer file (.lyr) generated.

**Attribute Query****Availability by Extension**

CrimeView
Attribute Query

FireView
Attribute Query

School Planner
Attribute Query

Attachment A

The Attribute Query routine selects features based on an attribute query. There is no Where? tab as a spatial query is not used.

The Attribute Query routine is the only [Query](#) routine that does not use a spatial query. Consequently, the routine is useful in selecting features that are not geocoded. Geocoding is the process of creating a geometric representation (such as a point) of a specific location from textual descriptive information, such as an address. Typically, not all addresses are geocoded therefore they do not have geometry (cannot be displayed on the map). However, these features are in the layer's attribute table. The Attribute Query routine selects those features that are both geocoded and not geocoded, provided that the feature satisfies the attribute query.

What?

The What? tab is used to specify the following query parameters:

- ***Query Layer***

Select the [Query Layer](#) from a list of point layers in the active data frame. The features in the Query Layer that satisfy the attribute query and date or time range are selected by the Attribute Query routine.

- Additional Query Layers

Select [Additional layers](#) that can be included with the Attribute Query routine.

- Attribute Query

Once the [Query Layer](#) is selected, the saved query groups registered to the Query Layer are displayed in the [Saved Queries](#) tree or columns.

When?

The When? tab is used to specify a [date or time range](#). This tab is only available if the [Query Layer](#) set in the What? tab has OmegaGIS date and time fields. For the School Planner product, this tab is not available since queries are always performed on a full year of student data.

Running the Attribute Query Routine

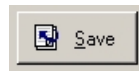
To run the Attribute Query routine, click the Finish button. The button is only enabled when all of the parameters for the routine are set. The required parameters for the Attribute Query routine require that:

Attachment A

- A [Query Layer](#) is set.

An attribute query and a date or time range are not required to run the routine.

When the Finish button is selected, the routine validates the parameters for the routine and then display a summary dialog. This dialog provides an overview of the Attribute Query routine parameters. Use the Back button to return to the query dialog to make edits to the Attribute Query routine. The Save button on the summary dialog allows the routine to be saved as a [Cyclical Report](#) and/or [Threshold Alert](#).



The "Display the routine summary dialog" option in the [OmegaGIS Setup](#) dialog controls whether the summary dialog is shown. The default option displays the summary dialog.

Results of the Attribute Query

When the Attribute Query routine is complete, the following events occur:

- The query dialog shrinks. To restore the query dialog, double click the icon in the upper right corner of the dialog. The [OmegaGIS Setup](#) dialog has a setting to hide rather than shrink the query dialog.
- The active data frame zooms to the selected features. The "Zoom to selection" option in the [OmegaGIS Setup](#) dialog controls this action.
- The selected features are displayed based on the "query result" option in the [OmegaGIS Setup](#) dialog. When a selection layer is created, the label information, including whether or not to display the labels, is copied from the original layer.

If no features are selected by the Attribute Query routine, the following events occur:

- The query dialog is maximized.
- A message box reports that the routine cannot be completed. If [additional query layers](#) are used, the number on the message box reads 7810306 otherwise the number reads 7810308.
- The OmegaGIS [definition expression](#) of the [Query Layer](#) and the [additional query layers](#) are removed.

Attachment A

- The visibility of the [Query Layer](#) reverts to its state before the Attribute query routine was run. If [additional query layers](#) were used all of the layers, including the Query Layer, will not be visible.

Tip:

- The selection layer must be exported to [permanent persist](#) the layer.

Date Updated: May 27, 2009



Within A Boundary

Availability by Extension

CrimeView	FireView	School Planner
Within A Boundary	Within A Boundary	Within A Boundary

The Within A Boundary routine selects features within one or more selected boundaries in addition to using an attribute query.

What?

The What? tab is used to specify the following:

- **Query Layer**

Select the [Query Layer](#) from the list of point layers in the active data frame. The features in the Query Layer that are within the selected boundaries and satisfy both the attribute query and date or time range are selected by the routine.

- Additional Query Layers

Select the [Additional layers](#) that can be included with the Within A Boundary routine.

- Attribute Query

Once the [Query Layer](#) is selected, the saved query groups registered to the Query Layer are displayed in the [Saved Queries](#) tree or columns.

Attachment A

Where?

The Where? tab is used to select the boundaries used for the spatial query when running the routine. There are two boundary types:

- Existing Boundary Layer

The features of an [existing boundary layer](#) are used to spatially query features. Select the boundary layer and then the features to include in the spatial query.

When editing a [Cyclical Report](#) or [Threshold Alert](#), if the By Pointing selection method has been used, the features in the boundary layer will be selected.

- User Defined Area

The [User Defined Area](#) boundary type is useful when there are no existing boundary layers that can be used to spatially query features.

When editing a [Cyclical Report](#) or [Threshold Alert](#) the user defined graphic element is created on the active data frame is automatically selected. To change the user defined boundary, delete the element and create a new one.

When?

The When? tab is used to specify a [date or time range](#). This tab is only available if the [Query Layer](#) set in the What? tab has OmegaGIS date and time fields. For School Planner this tab is not available as queries are performed on the full year of student data.

Running the Within A Boundary Routine

To run the Within A Boundary routine, click the Finish button. The Finish button is only enabled when all of the routine parameters are set. The required parameters for the Within A Boundary routine include:

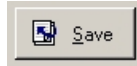
- A [Query Layer](#) must be set.
- When the [Existing Boundary Layer](#) boundary type is selected, the boundary layer is selected. When the selection method of By Field Value is used, at least one field value must be selected. When the By Pointing selection method is used, there is no check to ensure that features in the boundary layer are selected until the Finish button is clicked.

An attribute query and a date or time range are not required to run the Within a Boundary routine.

Attachment A

When the Finish button is selected, the routine validates the routine parameters and displays a summary dialog. The validation includes checking that there are features selected in the boundary layer when the [Existing Boundary Layer](#) boundary type is used with the By Pointing option. When the boundary type of [User-Defined Area](#) is used, the graphic element is checked.

The summary dialog provides an overview of the Within A Boundary routine parameters. Use the Back button to return to the query dialog to make edits to the Within a Boundary routine. The Save button on the summary dialog allows the routine to be saved as a [Cyclical Report](#) and [Threshold Alert](#).



The "Display the routine summary dialog" option in the [OmegaGIS Setup](#) dialog controls whether the summary dialog is shown. The default option displays the summary dialog.

Results of Within A Boundary

When the Within A Boundary routine is completed, the following events occur:

- The query dialog shrinks. To maximize the query dialog, double click the icon in the upper right corner. The [OmegaGIS Setup](#) dialog has a setting to hide rather than shrink the query dialog.
- The active data frame zooms to the boundary. The "Zoom to selection" option in the [OmegaGIS Setup](#) dialog controls this action.
- The selected features are displayed based on the "query result" option in the [OmegaGIS Setup](#) dialog. When a selection layer is created, the label information, including whether or not to display the labels, is copied from the original layer.
- The boundary layer will be visible.
- The features in the boundary layer that were used in the spatial query will be selected. The "Select features used as boundaries" option in the [OmegaGIS Setup](#) dialog controls this action.
- The features in the boundary layer will be labeled if that option was selected on the Where? tab. The style of the label is set in the [OmegaGIS Setup](#) dialog.

If no features are selected by the Within A Boundary routine, the following events occur:

Attachment A

- The query dialog is maximized.
- A message box reports that the routine cannot be completed. If [additional query layers](#) are used, the number on the message box reads 7810306 otherwise the number reads 7810308.
- The OmegaGIS [definition expression](#) of the [Query Layer](#) and the [additional query layers](#) are removed.
- The visibility of the [Query Layer](#) reverts to its state before the Within A Boundary routine was run. If [additional query layers](#) are used all of the layers, including the Query Layer, are set to invisible.
- The features in the boundary layer are selected, the "Select features used as boundaries" option in the [OmegaGIS Setup](#) dialog determines if the features are selected.
- The features in the boundary layer are labeled if that option is selected on the Where? tab. Use the [Clear All](#) to remove the labels.
- The active data frame zooms to the buffer. The "Zoom to selection" option in the [OmegaGIS Setup](#) dialog controls whether the zoom occurs or not.

Tip:

- The selection layer must be exported to [permanent persist](#) the layer.

Date Updated: May 27, 2009



Near An Address

Availability by Extension

CrimeView
Near An Address

FireView
Near An Address

School Planner
Near An Address

The Near An Address routine selects features based on their proximity to a location determined by a street address or street intersection.

Attachment A

The Near An Address routine uses address locators. Address locators are built as a method of geocoding which is the process of creating a geometric representation (such as a point) of a specific location from textual descriptive information, such as an address. An address locator is created by ArcGIS and is used to determine the location of an address or intersection. In ArcGIS versions previous to 9.0, the address locator was referred to as a geocoding service.

What?

The What? tab is used to specify the following query parameters:

- **Query Layer**

Select the [Query Layer](#) from the list of point layers in the active data frame. The features in the Query Layer that are within the designated buffer around the address or intersection and satisfy both the attribute query and date or time range are selected by the routine.

- Additional Query Layers

Select the [Additional layers](#) that can be included with the Near an Address routine.

- Attribute Query

Once the [Query Layer](#) is selected, the saved query groups registered to the Query Layer are displayed in the [Saved Queries](#) tree or columns.

Where?

The Where? tab is used to specify the address or intersection and buffer distance.

- Address

Enter the address or intersection used to select features based on their proximity.

When geocoding to large geographic regions, such as to an entire county, Omega recommends using an address locator style that supports zones. The zone provides additional information used to resolve ambiguity between addresses by identifying a region in which the address is located. The zone can be a ZIP code, city name or police beat. If the address locator has a style that uses zone, a zone text box is visible.



A screenshot of a software interface showing a text box labeled "Zone" with the value "92121" entered inside it.

Attachment A

When the address locator has a style that uses zone, the zone information entered is not used when the address contains an intersection connector. The intersection connectors are set with the address locator [properties](#) dialog and typically include "&" or "/". Click the [Geocoding Properties](#) button to view and edit the intersection connectors.

- Check address

To determine if the entered address or intersection can be found by the selected address locator, select the Check Address button. A message box states whether or not the address is geocoded. If the address is not geocoded attempt the following:

- Ensure that the address is spelled correctly.
- Alter the [geocoding properties](#) by reducing the spelling sensitivity or minimum match score.

- Address Locator

All of the address locators referenced by the ArcMap document are listed in the drop-down list. Select the address locator to use for the Near An Address routine.



Only valid address locators are available in the drop-down list. The most common reason for an invalid address locator is that its reference data, such as the street centerlines feature class, has been moved, renamed or deleted. Use ArcCatalog to determine the address locator issue.

Address locators based on the ESRI StreetMap are not currently supported and are not available in the drop-down list of address locators.

If the ArcMap document does not reference any address locators, there is a red exclamation mark beside the drop-down list of address locators.



To add or remove an address locator, select the Add/Remove button. This selection opens ArcMap's Address Locator Manager dialog to add additional address locators to the ArcMap document.

- Buffer Distance

The buffer distance is the radius around the selected address or intersection which is used in the spatial selection. The available measurement units for the buffer distance are Meters and Kilometers when using the Metric measurement system or Miles and Feet when the English measurement system is used. The measurement system is set in the [OmegaGIS Setup](#) dialog.

Attachment A

When the "Only at address (no buffer)" checkbox is selected, the buffer distance text box is disabled since there is no user defined buffer. The geocoded location is buffered 0.5 meters (1.64 feet) which creates the polygon that is required to make the spatial selection.

Only at address (no buffer)

- Geocoding Properties

To alter the properties of the address locator selected in the drop-down list, select the Geocoding Properties button. The button opens the Properties dialog for the address locator.

Any changes to the properties of the address locator, such as the spelling sensitivity, apply to the current ArcMap session only. When ArcMap closes, the changes to the geocoding properties are lost. Use ArcCatalog to make permanent changes to the properties of the address locator.

The parameters for the Near An Address routine may be saved as a [Cyclical Report](#) or [Threshold Alert](#). However, only the minimum match score and the spelling sensitivity geocoding properties are saved. Any edits to the minimum match score and spelling sensitivity address locator properties in ArcCatalog are not used when running a Cyclical Report or Threshold Alert. The Cyclical Report or Threshold Alert must be edited in order for the new geocoding properties to be saved.

When?

The When? tab is used to specify a [date or time range](#). This tab is only available if the [Query Layer](#) set in the What? tab has OmegaGIS date and time fields. For School Planner, this tab is not available as all queries are performed on the full year of student data.

Running the Near An Address Routine

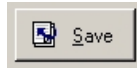
To run the Near An Address routine, click the Finish button. The Finish button is only enabled when all of the routine parameters are set. The required parameters for the Near An Address routine include:

- A [Query Layer](#) is set.
- An [address](#) is entered. If the address locator uses zone information, the zone does not have to be entered for the Finish button to be enabled.
- An [address locator](#) is selected.

Attachment A

An attribute query and a date or time range are not required to run the Near An Address routine.

When the Finish button is selected, the routine will validate the routine parameters and then display a summary dialog. This dialog provides an overview of the Near An Address routine parameters. Use the Back button to return to the query dialog to make edits to the Near An Address routine. The Save button on the summary dialog allows the routine to be saved as a [Cyclical Report](#) and/or [Threshold Alert](#).



The "Display the routine summary dialog" option in the [OmegaGIS Setup](#) dialog controls whether the summary dialog is shown. The default option displays the summary dialog.

Results of Near An Address

When the Near An Address routine is complete, the following events occur:

- The query dialog shrinks. To restore the query dialog, double click the icon in the upper right corner. The [OmegaGIS Setup](#) dialog has a setting to hide rather than shrink the query dialog.
- The active data frame zooms to the buffer around the address or intersection. The "Zoom to selection" option in the [OmegaGIS Setup](#) dialog controls this action.
- The selected features are displayed based on the "query result" option in the [OmegaGIS Setup](#) dialog. When a selection layer is created, the label information, including whether or not to display the labels, is copied from the original layer.
- The buffer is drawn around the address. The buffer is an element in the OmegaGIS buffer annotation group.
- The address is labeled if that option is selected on the Where? tab. The style of the label is set in the [OmegaGIS Setup](#) dialog.

If no features are selected by the Near an Address routine, the following events occur:

- The query dialog is maximized.
- A message box reports that the routine cannot be completed. If [additional query layers](#) are used, the number on the message box reads 7810306 otherwise the number reads 7810308.

Attachment A

- The OmegaGIS [definition expression](#) of the [Query Layer](#) and the [additional query layers](#) are removed.
- The visibility of the [Query Layer](#) reverts to its state before the Near an Address routine was run. If [additional query layers](#) were used all of the layers, including the Query Layer, they will not be visible.
- The buffer around the address is drawn and the active data frame zooms to the buffer. The "Zoom to selection" option in the [OmegaGIS Setup](#) dialog controls whether the zoom occurs. Use the [Clear All](#) to remove the Near an Address buffer.

Tip:

- The selection layer must be exported to [permanent persist](#) the layer.

Date Updated: May 27, 2009



Near A Feature

Availability by Extension

CrimeView	FireView	School Planner
Near A Feature	Near A Feature	Near A Feature

The Near A Feature routine selects features based upon their proximity to one or more selected features in addition to an attribute query. Features can be point (e.g. schools or banks), line (e.g. streets or rivers) or polygon (e.g. parks or report districts).

What?

The What? tab is used to specify the following query parameters:

- ***Query Layer***

Select the [Query Layer](#) from the list of point layers in the active data frame. The features in the Query Layer that are within the buffer around the selected features and satisfy both the attribute query and date or time range are selected by the Near a Feature routine.

Attachment A

- Additional Query Layers

Select [Additional layers](#) that can be included with the Near A Feature routine.

- Attribute Query

Once the [Query Layer](#) is selected, the saved query groups registered to the Query Layer are displayed in the [Saved Queries](#) tree or columns.



Where?

The Where? tab is used to specify the [feature layer](#), [selection method](#) and the [buffer distance](#).

- Feature Layer

Select the feature layer from the drop-down list. The criteria used to populate the list of feature layers includes:

- The layer must be in the active data frame.
- The layer must be valid; the data source of the layer is not missing. When the data source is missing the layer has a red exclamation mark in the table of contents.

  2002 Part I Crimes


- The layer must have a geometry type of point, polygon or line.
- If the layer was generated by an OmegaGIS routine, such as a [composite layer](#) or [density map](#), an option in the [OmegaGIS Setup](#) dialog must be set to include these layers.

- Selection Method

There are three methods available which can be used to select features for the Near A Feature Routine:

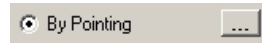
Use Selected Features

This selection method is only available if the layer has selected features when the query dialog is loaded. The number of selected features found in the feature layer are displayed beside the option.

 Use selected features (3)

Attachment A**By Pointing**

The "By Pointing" selection method allows interactive selection of the layer's features to be used in the spatial query. With this option selected, click the ellipses button to shrink the dialog, make the feature layer visible and ensure that the feature layer is the only selectable layer in the active data frame.



Click the feature to be selected. To select multiple features, hold down the SHIFT key and click the other features. Alternatively, select features by dragging a box around a group of features. All of the features touching or within the box are selected.

When the selection is complete, double click the flashing icon in the upper right corner of the dialog. The dialog expands to its normal size and the selectability of the layers returns to its original state before the dialog was collapsed.

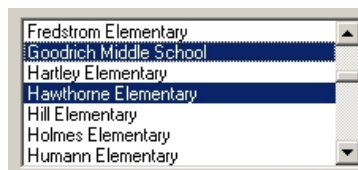
By Field Value

The "By Field Value" selection method selects features in the layer, such as a police beat, fire district or school district, based on the features attribute value.

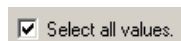
From the Field Name drop-down listbox, select the field from the feature layer that has values that are to be used to identify the features for the spatial query. The field should contain values that uniquely identify features in the layer, such as a school name. If an OmegaGIS default field is specified in the metadata for the feature layer, this field will automatically be selected. The OmegaGIS default field is set with the [OmegaGIS Metadata Editor](#).



From the list of Field Values, select the values that represent the features to use in the feature layer. To select more than one value, hold down the CTRL key. To un-select a value from the list, hold down the CTRL key and select it again.



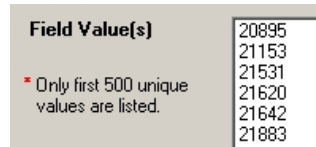
To select all of the field values and use all of the features in the layer, check the "Select all values" checkbox.



Attachment A

The Field Values list contains a unique list of values. In an effort to improve the performance of the OmegaGIS application, a predefined number of features in the feature layer are used to determine the unique values. The number of features used to search for unique values is set in the [OmegaGIS Setup](#) dialog. For layers with a large number of features from which to search, select the Complete List button to sample each of the features found in the layer for unique values.

There is a limit to the number of unique values displayed in the Field Values list. This limit is set in the [OmegaGIS Setup](#) dialog. When the limit of unique values is reached, a warning is displayed to the left of the list. The maximum number of unique values that can be displayed in the Field Values list is 30,000. If this becomes an issue, use the By Pointing selection method.



- Buffer Distance

The buffer distance is the radius around the selected feature which is used in the spatial selection. The available measurement units for the buffer distance are Meters and Kilometers when using the Metric measurement system or Miles and Feet when the English measurement system is used. The measurement system is set in the [OmegaGIS Setup](#) dialog.

When the "Only at feature (no buffer)" checkbox is selected, the buffer distance text box is disabled since there is no user defined buffer. The feature is buffered 0.5 meters (1.64 feet) which creates a polygon that is required to make the spatial selection.

**When?**

The When? tab is used to specify a [date or time range](#). This tab is only available if the [Query Layer](#) set in the What? tab has OmegaGIS date and time fields. For School Planner, this tab is not available as queries are always performed on the full year of student data.

Running the Near a Feature Routine

To run the Near a Feature routine, click the Finish button. The Finish button is only enabled when all of the parameters for the routine are set. The required parameters for the Near a Feature routine include:

- A [Query Layer](#) is set.

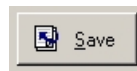
Attachment A

- The [feature layer](#) is selected.
- When the selection method of By Field Value is used, at least one field value must be selected. When the By Pointing or Use selected features selection methods are used, there is no check to ensure that features are selected in the feature layer until the Finish button is clicked.

An attribute query and a date or time range are not required to run the Near a Feature routine.

When the Finish button is selected, the routine validates the parameters and then displays a summary dialog. The validation includes checking that there are features selected in the [feature layer](#) when either the By Pointing or Use selected features options is used.

The summary dialog provides an overview of the parameters for the Near A Feature routine. Use the Back button to return to the query dialog to make edits to the Near A Feature routine. The Save button on the summary dialog allows the routine to be saved as a [Cyclical Report](#) and [Threshold Alert](#).



The "Display the routine summary dialog" option in the [OmegaGIS Setup](#) dialog controls whether the summary dialog is shown. The default option displays the summary dialog.

Results of Near A Feature

When the Near a Feature routine is completed, the following events occur:

- The query dialog shrinks. To maximize the query dialog, double click the icon in the upper right corner. The [OmegaGIS Setup](#) dialog has a setting to hide rather than shrink the query dialog.
- The active data frame zooms to the extent of the buffer(s). The "Zoom to selection" option in the [OmegaGIS Setup](#) dialog controls this action.
- The selected features are displayed based on the "query result" option in the [OmegaGIS Setup](#) dialog. When a selection layer is created, the label information, including whether or not to display the labels, is copied from the original layer.
- The [feature layer](#) is visible.

Attachment A

- The features in the [feature layer](#) used in the spatial query are selected. The "Select features used as boundaries" option in the [OmegaGIS Setup](#) dialog controls this action.
- The features in the [feature layer](#) are labeled if that option is selected on the Where? tab. The style of the label is set in the [OmegaGIS Setup](#) dialog.

If no features are selected by the Near A Feature routine, the following events occur:

- The query dialog is maximized.
- A message box reports that the routine cannot be completed. If [additional query layers](#) are used, the number on the message box reads 7810306 otherwise the number reads 7810308.
- The OmegaGIS [definition expression](#) of the [Query Layer](#) and the [additional query layers](#) are removed.
- The visibility of the [Query Layer](#) reverts to its state before the Near A Feature routine was run. If [additional query layers](#) were used all of these layers, including the Query Layer, will not be visible.
- The features in the [feature layer](#) are selected, the "Select features used as boundaries" option in the [OmegaGIS Setup](#) dialog determines if the features are selected.
- The features in the [feature layer](#) are labeled if that option is selected on the Where? tab. Use the [Clear All](#) to remove the labels.
- The active data frame zooms to the buffer around the selected features. The "Zoom to selection" option in the [OmegaGIS Setup](#) dialog controls whether the zoom occurs.

Tip:

- The selection layer must be exported to [permanent persist](#) the layer.

Date Updated: May 27, 2009

Density Maps


There are three different routines that may be run from the Density dialog. Use the buttons along the top of the dialog to choose the routine. The selected routine button will be in colour and the label at the top right will display the name of the routine.

Attachment A

When a different routine is selected, the What? tab will become active and the How? tab will change based on the routine selected.

 **D** [Density Map](#)

The Density Map routine creates a *choropleth* map using either the count of features or density of features (count of features / area) in an existing boundary layer.

 **H** [Hot Spot Map](#) (*Spatial Clustering in School Planner*)

The Hot Spot routine creates a raster layer that displays the concentration of features. ArcGIS Spatial Analyst is required to run the routine.

 **R** [Repeat Calls](#) (*Student Concentrations in School Planner*)

The Repeat Calls routine creates a layer that reveals places that have numerous features at the same location.

Tip

- When the Density dialog is opened, the routine that was last used is selected. If no Density routine was used, the Density Map routine is selected.



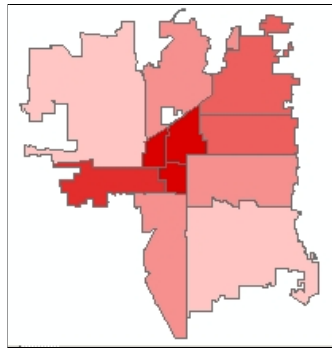
About Density Map Routine

Availability by Extension

CrimeView	FireView	School Planner
Density Map	Density Map	Density Map

A choropleth map symbolizes the magnitudes of statistics as they occur within boundaries, such as Police Beats or School Districts. The Density Map routine creates a choroplethic map of either the count of features or density of features (count of features / area) in an existing boundary layer.

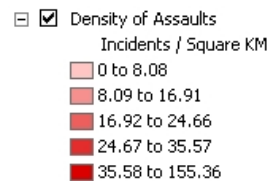
The Density Map layer, created by the routine, provides a way to view the variability of features in the boundary layer. If the boundary layer has large areas, the Density Map routine will process quickly but the spatial variation of the incident tends to be reduced or averaged out. On the other hand, if the boundary layer has small areas, the spatial variation is preserved at the cost of increased processing time for the routine.

Attachment A

The layers generated by the Density Map routine can have a [Crystal Report](#) associated with them. The Density Map Crystal Report provides a statistical summary of the count and density values in order to identify statistical outliers or potential problem areas.

Classification of Layer

The count or density field for the Density Map layer are broken into arbitrary classes and these classes are used in the legend for the Density Map layer. The Jenks Natural Breaks statistical formula is used to inspect the data and determine the class breaks. This method attempts to minimize the variance within the class and to maximize the variance between the classes. Hence, the natural breaks method highlights the 'natural grouping'.



The classes are related to the data, as opposed to predefined class breaks. Consequently, the class breaks will change for each Density Map layer created.

These class breaks can be edited after the routine is completed by using the Symbology tab in the Density Map layer's Properties dialog.

**Create Density Map Layer**

There are four tabs available that contain options and settings for creating and displaying a [Density Map](#) layer. The tabs included [What?](#), [How?](#), [Where?](#) and [When?](#) School Planner does not support the When? tab, as all queries are expected to be made on the full year of student data.

Attachment A**What?**

The *What?* tab is used to specify the following query parameters:

- **Query Layer**

Select the [Query Layer](#) from the list of point layers in the active data frame. The incidents in the Query Layer that satisfy both the attribute query and date or time range are used to generate the Density Map.

- Additional Query Layers

Select [Additional layers](#) that can be included with the Density Map routine.

- Attribute Query

Once the [Query Layer](#) is selected, the saved query groups registered to the Query Layer are displayed in the [Saved Queries](#) tree or columns.



How?

The *How?* tab includes settings that control the way in which the Density Map is created and displayed.

- Boundary Layer

From the drop-down list, select the polygon layer to be used as the boundary layer. The features that satisfy both the attribute query and the date or time range will be summarized for each feature in the boundary layer. The criteria used to populate the list of boundary layers includes:

- The layer is in the active data frame.
- The layer is valid; this means the data source of the layer is not missing. When the data source is missing the layer has a red exclamation mark in the table of contents.

  2002 Part I Crimes

- The layer must have a geometry type of polygon.

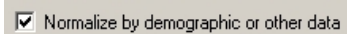
Attachment A

- There is an option in the [OmegaGIS Setup](#) dialog that controls whether to exclude layers created by OmegaGIS routines in the list of boundary and query layers. An example of a layer created by an OmegaGIS routine might be a [density map](#). This layer can be excluded or included in the boundary layer list by toggling the setting in the OmegaGIS Setup dialog. By default, layers created by OmegaGIS routines are not included in the boundaries list.

- Normalize Field

To normalize the summarized feature data, select the "Normalize by demographic or other data" checkbox and then the field to use from the drop-down list. This list contains numeric fields from the boundary layer.

The "Shape_Length" and "Shape_Area" fields found with layers stored in a personal geodatabase or the "Shape.Len" and "Shape.Area" fields found with layers stored in ArcSDE are not available in the list of normalize fields.



Normalizing divides the count of the summarized features by the value of the normalization field for that boundary feature; the result is used in the creation of the density map legend.

Normalized Value = (Count of Features / Normalize Field Value)

Normalizing data minimizes differences in values based on the numbers of features in each area. For example, dividing a count of emergency medical incidents by the number of persons over 65 years of age in each census tract will minimize the effect on the incident density distribution map resulting from concentrated elderly population.

- New Layer Name

Enter the name for the new density layer which is used when the density map layer is added to the active data frame's table of contents.

- Color Scheme

From the drop-down list, select the color ramp that is used to generate the legend of the new density map. These color ramps are stored in the [OmegaGIS.STYLE](#) file.



- Classify By

There are two options that determine how the new density map legend will be classified:

Attachment A

Density

The count of features are divided by the area of the boundary feature. When the Metric measurement system is set in the [OmegaGIS Setup](#) dialog, the density is calculated as feature per square kilometer. When the English measurement system is used, the density is calculated as features per square mile.

The Density option is not enabled when the "Normalize by demographic or other data" checkbox is selected.

Count

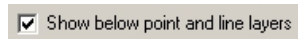
The count of the features found in the boundary feature are used.

- Options

Two options are available in controlling the placement and look of the new density map.

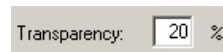
Show below point and line layers

Use the "Show below point and line layers" checkbox to have the new density map layer placed below all point and line layers in the active data frame. By default, the new density map layer will be added at the top of the table of contents and may obscure point and line layers below it.



Transparency

The transparency setting can also be used to ensure that points and lines below the new density map layer will not be obscured. Set the percentage of transparency for the new density layer, where 0% means that the layer is opaque and 100% means that the layer is invisible. This transparency value can also be changed later by using the Display tab in the Layer Properties dialog. The default transparency value is 20%.



Where?

The *Where?* tab provides options to narrow down the number of features in the boundary layer used in the creation of the density map. The *Where?* tab is only enabled when the "Subset by boundary" checkbox is selected on the *How?* tab.

Attachment A

Select the features in the [boundary layer](#) that are to be used in the spatial query. The "Select all values" checkbox is not available on the *Where?* tab; if all of the features in the boundary layer are to be used then do not use the subset by boundary option.

When editing a [Cyclical Report](#) and the By Pointing selection method has been selected, the boundary features are selected.

When?

The *When?* tab is used to specify a [date or time range](#). This tab is only available if the [Query Layer](#) set in the *What?* tab has OmegaGIS date and time fields. When using Density Map in School Planner, this tab is not available as all queries are made on the entire school year.

Running the Density Map Routine

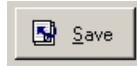
To create the density map, click the Finish button. The Finish button is only enabled when all of the parameters for the routine are set. The required parameters for the Density Map routine require that:

- A [Query Layer](#) is set.
- The boundary layer is selected.
- when the "Normalize by demographic or other data" option is selected, a field in the normalize fields drop-down list is selected.
- When the "Subset by boundary" option is selected and the By Field Value selection method is used, the field name drop-down list has a field selected and at least one field value is selected. When the By Pointing selection method is used, there is no check to ensure that features are selected in the boundary layer until the Finish button is clicked.

An attribute query and a date or time range are not required to run the Density Map routine.

When the Finish button is selected, the routine validates the parameters and then displays a summary dialog. The validation includes checking that there are features selected in the boundary when the By Pointing option is used.

The summary dialog provides an overview of the parameters for the Density routine. Use the Back button to return to the query dialog to make edits to the routine. The Save button on the summary dialog allows the routine to be saved as a [Cyclical Report](#).



The "Display the routine summary dialog" option in the [OmegaGIS Setup](#) dialog controls whether the summary dialog is shown. The default option displays the summary dialog.



Results of Density Map Routine

This section describes the results of the Density Map routine and is divided into the following topics:

[Results of Routine](#)

[DensityMap.MDB](#)

[Density Map Layer](#)

Results of Routine

When the Density Map routine is successfully completed, the following events occur:

- The density dialog shrinks. To maximize the density dialog, double click the icon in the upper right corner. The [OmegaGIS Setup](#) dialog has a setting to hide rather than shrink the density dialog.
- The extent of the active data frame is changed to the extent of the newly created Density Map layer plus a 5% buffer.
- The [Query Layer](#) and any [additional query layers](#) that are used to generate the Density Map layer have the following done to them:
 - Layer has visibility turned off.
 - The OmegaGIS [definition expression](#) is removed from the layer.
 - The selected features are cleared.
- The boundary layer will have following done:
 - Any selected features will be cleared. The "Select features used as boundaries..." option in the [OmegaGIS Setup](#) dialog does not apply to the Density Map routine.

Attachment A

- The visibility of the layer is not altered. If the boundary layer was visible when the Density Map routine is run then it will be visible when the routine is completed.

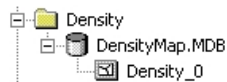
If no incidents are selected by the Density Map routine, the following events occur:

- The density dialog is maximized.
- A message box reports that the routine cannot be completed. If [additional query layers](#) are used, the number on the message box reads 7810306 otherwise the number reads 7810434.
- The OmegaGIS [definition expression](#) of the [Query Layer](#) and the [additional query layers](#) are removed.
- The visibility of the [Query Layer](#) is the same as before running the Density Map routine. If [additional query layers](#) are used, all of the layers, including the Query Layer, are not visible.

DensityMap.MDB

During the running of the routine, a new feature class is generated in a personal Geodatabase. The Density Map layer is based on this feature class.

- The Geodatabase is named DensityMap.MDB and is located in the "\Density" folder in the project workspace.



- The DensityMap.MDB is created dynamically by the Density Map routine. If the Geodatabase is not present it is created when the Density Map routine is run.
- The feature class has all of the boundary layer fields plus two new fields that are created by the routine.

OmegaGIS_Count

This field contains the number of features that are found in the boundary.

OmegaGIS_Density

The density (count of features/ area) is in this field. The area is in square Kilometers or in square miles, depending on the measurement system selected in the [OmegaGIS Setup](#) dialog.

The "Shape_Area" field is not used in the calculation of the OmegaGIS_Density field. The "Shape_Area" field is created and maintained by the Geodatabase and the values in this field are in the units of the spatial reference of the feature class which may not be in Kilometers or Miles.

- When the feature class in the DensityMap.MDB is no longer in the data frame, it is deleted by the [OmegaGIS Project Exit](#).

Tip:

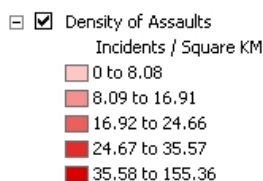
- To [permanently persist](#) the feature class created from a density routine, export the feature class to a different personal Geodatabase.

Density Map Layer

The Density Map routine adds a layer to the active data frame whose data source is from a feature class in the [DensityMap.MDB](#). The Density Map layer has the following settings:

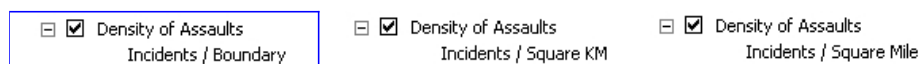
- Class Breaks

The graduated colors renderer is used with the Jenk's [Natural Breaks](#) statistical formula that is used to determine the class breaks used in the legend. While five class breaks are used by default, the number of classes is automatically reduced if the data does not support being broken into five classes.



- Legend Heading

The heading of the legend in the table of contents changes based on how the layer was [classified](#). The heading can be altered by double-clicking the text which makes the text editable.



Attachment A

- Round Values

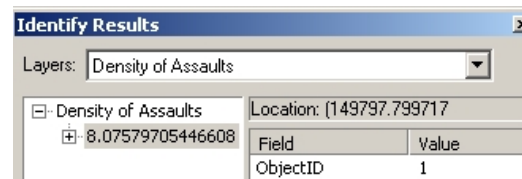
When using the Density classify method, the values for the class breaks in the legend are rounded to two decimal places.

- Labels

The label properties, the label field or the label expression and the text symbol, are copied from the boundary layer.

- Primary Display Field

The primary display field is set to either the OmegaGIS_Count or OmegaGIS_Density field; based on which was selected to [classify](#) the layer. The primary display field is used with the ArcMap Identify tool. The value of the field is shown on the right side of the Identify Results dialog rather than scrolling through the list of field values.



- Color Ramp

The color ramp used with the layer is from the [OmegaGIS.STYLE](#) and is set to the layer.



About Hot Spot / Spatial Clustering Routine

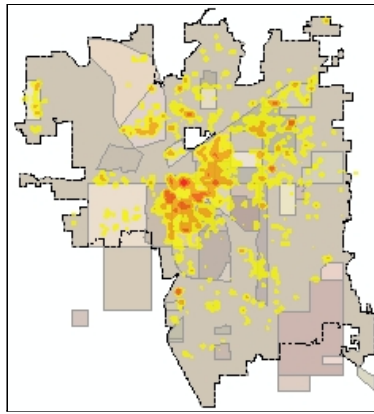
Availability by Extension

CrimeView
Hot Spot

FireView
Hot Spot

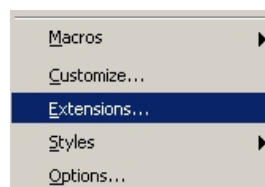
School Planner
Spatial Clustering

The Hot Spot routine (Spatial Clustering in School Planner) creates a raster layer that displays the concentration of features. The ArcGIS Spatial Analyst extension is required to run the routine.

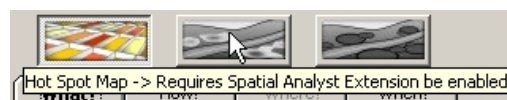
Attachment A**Spatial Analyst Extension**

There are two main types of Geographic Information System (GIS) data, vector and raster. Vector data takes a study area, such as a city, and converts the features into points, lines and polygons. On the other hand, raster data converts the study area into a regular grid of cells. Each cell contains a single value.

Spatial Analyst is an extension to ArcGIS and allows for the creation, querying and analysis of cell-based raster layers. OmegaGIS will automatically enable the Spatial Analyst extension, if licensed from ESRI, when the [Density](#) dialog opens. The "all extensions used with OmegaGIS routines..." option in the [OmegaGIS Setup](#) dialog controls the enabling of the Spatial Analyst extension. To manually enable the extension, from the Tools pull-down menu in ArcMap select Extensions and from the dialog select the Spatial Analyst extension; there is a message box that states if the extension is not licensed from ESRI.



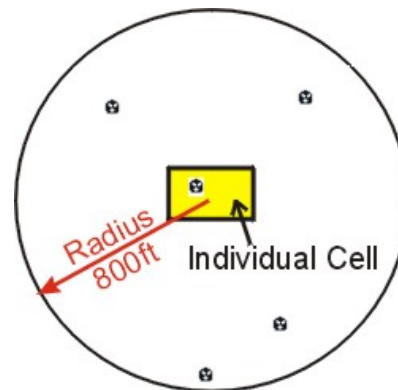
If the Spatial Analyst extension is not enabled, when the routine button is selected a message box (780026) will report that the routine cannot be run without the Spatial Analyst extension enabled. Additionally, the tool tip over the routine button states that the Spatial Analyst extension is not enabled.

**Creating Raster Layers**

Attachment A

The resulting layer from the Hot Spot routine (Spatial Clustering in School Planner) is a raster. A raster is made up of individual cells that all have the same size and a single value.

The Hot Spot routine (Spatial Clustering) creates the raster from the point data using the Density function in Spatial Analyst. The value assigned to each cell is based on the frequency of features found in proximity to the cell. By default, the cell size is 75 meters by 75 meters when using the Metric measurement system or 250 feet by 250 feet when using the English measurement system. The search distance, which is the radius measured from the center of the cell that is used to locate nearby features, the default value is 250 meters or 800 feet.

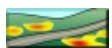


The density type of Kernel is used as opposed to the Simple density type. With the Simple density type, the value of each cell is calculated by counting the number of points found within the radius and that value is divided by the area of the search radius. The Kernel type works the same as Simple, except points lying nearest the center of the cell are given a greater weight. If a population field is identified, the values in that field are used to weight the points in the cell value scoring.

The result of the Hot Spot Routine (Spatial Clustering) is a raster layer that represents a continuous density surface of features.

Tip

- The cell size should be small enough to capture the detail but large enough to limit the amount of storage space on disk that the raster requires and improve performance of the routine. The cell size is depend on the study area and data accuracy.



Create Hot Spot / Spatial Clustering Layer

There are four tabs available that contain options and settings for creating and displaying a Hot Spot (Spatial Clustering) layer. The tabs included [What?](#), [How?](#), [Where?](#) and [When?](#) The term Hot Spot is used within the CrimeView and FireView products, while Spatial Clustering is the term used within the School Planner product. School Planner does not support the When? tab, as all queries are expected to be made on the full year of student data.

What?

Attachment A

The What? tab is used to specify the following query parameters:

- **Query Layer**

Select the [Query Layer](#) from the list of point layers in the active data frame. The features in the Query Layer that satisfy both the attribute query and date or time range are used to generate the Hot Spot layer.

- Additional Query Layers

Select [additional layers](#) that can be included with the Hot Spot routine.

- Attribute Query

Once the [Query Layer](#) is selected, the saved query groups registered to the Query Layer are displayed in the [Saved Queries](#) tree.

How?

The How? tab includes settings that control the way in which the Hot Spot layer is generated and displayed.

- New Layer Name

Enter the name for the new hot spot (spatial clustering) layer which is used when the layer is added to the active data frame's table of contents.

- Color Scheme

From the drop-down list, select the color ramp that is used to generate the legend of the new hot spot (spatial clustering) map. These color ramps are stored in the [OmegaGIS.STYLE](#) file.

- Population Field

A population field is used for weighting each feature when generating the [raster](#).

The population field list contains all of the numeric fields in the [Query Layer](#). The "Shape_Length" and "Shape_Area" fields found with layers stored in a personal geodatabase or the "Shape.Len" and "Shape.Area" fields found with layers stored in ArcSDE are not available in the population field list.

Select "< Do not use population field >" item in the list to not use a population field.

Attachment A

- Layer Extent

Set the spatial extent of the new raster. The list contains "< Same as selected features >", "< Same as current extent >", "< Same as data frame >" and all valid layers in the active data frame. The list is disabled when the "Subset by boundary" option is selected as the extent of the selected boundary layer features are used.

When the "< Same as selected features >" option is selected, the extent of the selected features is expanded by 10% to prevent the raster from cutting off a hot spot.

- **Raster Options**

There are two options that can be set that control how the raster is generated.

Cell Size

Specifies the size of individual cells in the [raster](#). The smaller the size of the cell the longer time it will take to generate the raster. The default cell size is 75 meters when the Metric measurement system is set in the [OmegaGIS Setup](#) dialog with a valid range of 3 to 1000 meters. The default cell size is 250 feet when the English measurement system is used with a valid range of 10 to 3280 feet.

If a cell size is entered outside the valid range, the default value for that measurement system will be used.

Search Distance

The search distance is the radius around each [cell](#) that is searched for features. The default search distance is 250 meters when the Metric measurement system is set in the [OmegaGIS Setup](#) dialog with a valid range of 5 to 4000 meters. The default search distance is 800 feet when the English measurement system is used with a valid range of 15 to 13200 feet.

If the search distance provided is outside the valid range, the default value for that system of measure will be used. Furthering this, the search distance must be 1.5 times greater than the cell size, this is to ensure that the search distance is large enough to include the entire cell. If this is not the case, then the search distance value is automatically increased while the routine is run. The metadata of the hot spot (spatial clustering) map contains information on the cell size and search distance that were used to generate the raster.

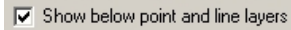
Select the Reset button to return to cell size and search distance to the default values.

- Options

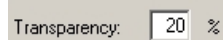
Two options are available in controlling the placement and look of the new hot spot (spatial clustering) layer.

Show below point and line layers

Use the "Show below point and line layers" checkbox to have the new hot spot layer placed below all point and line layers in the active data frame. By default, the new hot spot layer will be added at the top of the table of contents and may obscure point and line layers below it.

Attachment A**Transparency**

The transparency setting can also be used to ensure that points and lines below the new hot spot (spatial clustering) layer will not be obscured. Set the percentage of transparency for the new hot spot layer, where 0% means that the layer is opaque and 100% means that the layer is invisible. This transparency value can also be changed later by using the Display tab in the Layer Properties dialog. The default transparency value is 20%.

**Where?**

The Where? tab is used to select boundaries for a spatial query when running the routine. The Where? tab is only enabled when the "Subset by boundary" checkbox is selected on the How? tab. There are two boundary types:

- Existing Boundary Layer

The features of an [existing boundary layer](#) are used to spatially query features. Select the boundary layer and then features to include in the spatial query.

When editing a [Cyclical Report](#) and the By Pointing selection method has been used, the features in the boundary layer will be selected.

- User Defined Area

The [User Defined Area](#) boundary type is a useful when there are no existing boundary layers that can be used to spatially query features.

When editing a [Cyclical Report](#) the user defined graphic element will be created on the active data frame and it is selected. To change the user defined boundary, delete the element and create a new one.

When?

The When? tab is used to specify a [date or time range](#). This tab is only available if the [Query Layer](#) set in the What? tab has OmegaGIS date and time fields. This tab is not available in School Planner where it is necessary to create queries on the entire year

Attachment A

of student data.

Running the Hot Spot / Spatial Clustering Routine

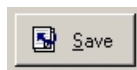
To create the Hot Spot (Spatial Clustering) layer, click the Finish button. The Finish button is only enabled when all of the parameters for the routine are set. The required parameters for the Hot Spot routine include:

- A [Query Layer](#) is set.
- When the "Subset by boundary" option is selected and [existing boundary layer](#) is used at least one field value has been selected when the By Field Value selection method is used. When the By Pointing selection method is used, there is no check to ensure that features are selected in the boundary layer until the Finish button is clicked.

An attribute query and a date or time range are not required to run the Hot Spot (Spatial Clustering) routine.

When the Finish button is selected, the routine validates the parameters and then displays a summary dialog. The validation includes checking that there are features selected in the boundary when the By Pointing option is used when subsetting by boundary. When the boundary type of [User-Defined Area](#) is used, the graphic element is checked.

The summary dialog provides an overview of the parameters for the Hot Spot (Spatial Clustering) routine. Use the Back button to return to the query dialog to make edits to the routine. The Save button on the summary dialog allows the routine to be saved as a [Cyclical Report](#).



The "Display the routine summary dialog" option in the [OmegaGIS Setup](#) dialog controls whether the summary dialog is shown. The default option displays the summary dialog.

Date Updated: May 27, 2009



Results of Hot Spot / Spatial Clustering Routine

This section describes the results of the Hot Spot (Spatial Clustering in School Planner) routine and is divided in the following topics:

[Results of Routine](#)

Attachment A[Raster](#)[Hot Spot \(Spatial Clustering\) Layer](#)**Results of Routine**

When the Hot Spot (Spatial Clustering) routine is successfully completed, the following events occur:

- The density dialog shrinks. To maximize the density dialog, double click the icon in the upper right corner. The [OmegaGIS Setup](#) dialog has a setting to hide rather than shrink the density dialog.
- The extent of the active data frame is changed to the extent of the new Hot Spot (Spatial Clustering) layer plus a 5% buffer.
- The [Query Layer](#) and any [additional query layers](#) that are used to generate the Hot Spot (Spatial Clustering) layer have the following done to them:
 - Layer has visibility turned off.
 - The OmegaGIS [definition expression](#) is removed from the layer.
 - The selected features are cleared.
- If a boundary layer is used as a spatial query, the boundary layer has the following done:
 - The features used in the spatial query will be selected. The "Select features used as boundaries..." option in the [OmegaGIS Setup](#) dialog controls this option.
 - The boundary layer will be visible.

If no features are selected by the Hot Spot (Spatial Clustering) routine, the following events occur:

- The density dialog is maximized.
- A message box reports that the routine can not be completed. If [additional query layers](#) are used, the number on the message box reads 7810306 otherwise the number reads 7810439.
- The [Query Layer](#) and the additional query layers have their OmegaGIS [definition expression](#) removed.
- The visibility of the [Query Layer](#) will be the same as before running the Hot Spot (Spatial Clustering) routine. If [additional](#)

Attachment A

[query layers](#) were used, all of the layers, including the Query Layer, will not be visible.

- The active data frame does not zoom.

Raster

The Hot Spot (Spatial Clustering) routine creates a raster layer. The raster is stored in the "HotSpot" folder in the [project workspace](#). This raster is permanent and will be automatically deleted from disk when it is no longer referenced by ArcMap by the Omega project clean up routine.



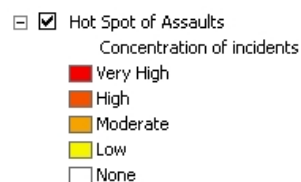
Hot Spot / Spatial Clustering Layer

The Hot Spot (Spatial Clustering) routine adds a layer to the active data frame. The Hot Spot (Spatial Clustering) layer has the following settings:

- **Class Breaks**

The classified renderer is used with the Jenk's Natural Breaks statistical formula which determines the class breaks used in the legend. While five class breaks are used by default, the number of classes is automatically reduced if the data does not support being broken into five classes.

The label of the class breaks does not use the range of the cell values but rather categories describing the concentration of the features.



- **Legend Heading**

The heading of the legend in the table of contents states "Concentration of incidents" or "Concentration of Students" in School Planner. The heading may be altered by double clicking the text which makes the text editable.

- *Color Ramp*

The color ramp used with the layer is from the [OmegaGIS.STYLE](#). However, since the lowest class break does not use the color ramp for its symbology, the color ramp displayed on the Symbology tab in the Layer Properties dialog is not the OmegaGIS color ramp.

- *Resampling Technique*

The **Bilinear Interpolation** resample technique is used to display the layer since the raster created by the routine contains [continuous data](#). This technique gives a smooth appearance to the data.



About Repeat Calls/Student Concentrations Routine

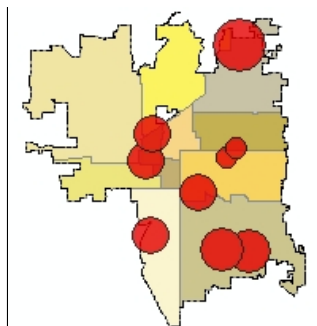
Availability by Extension

CrimeView
Repeat Calls

FireView
Repeat Calls

School Planner
Student Concentrations

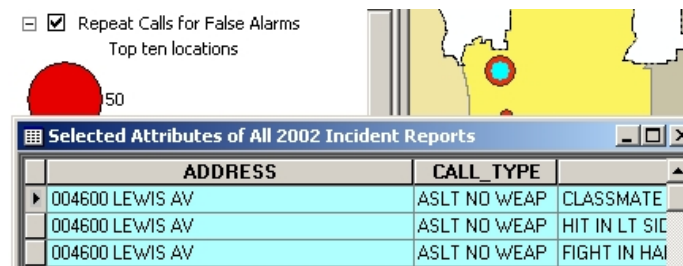
The Repeat Calls / Student Concentrations routine creates a layer that reveals the places with multiple features occurring at the same location. This routine calculates the repeat calls (student concentrations) spatially and does not use any attribute information to determine repeating locations.



There is the ability to register a [Crystal Report](#) to a Repeat Calls (Student Concentrations) layer that summarizes the features found at the same location.

Attachment A

The Repeat Calls (Student Concentrations) [Identify tool](#) is used to identify the features at a specific location.

**Known Issue**

There is a known issue with the Repeat Calls routine and migrating to the high precision spatial reference. ArcGIS 9.2 introduced the ability to store coordinates in high precision. Compared to low precision, high precision storage allows one to store coordinates closer together.

When the source query layer is updated to use the high precision spatial reference, the location of existing features does not change. However, new features that are added to the layer that have the same address as before the update of the spatial reference, may now have a different location. Since the Repeat Calls routine uses the geometry of the features to determine repeat calls locations, the results of the routine may not be accurate after the upgrade in spatial reference.

If this issue is encountered, the only resolution is to import the source query layer again so that features with the same address will share the same location. It is only necessary to update those features that were created in low precision.



Create Repeat Calls / Student Concentrations Layer

There are four tabs available that contain options and settings for creating and displaying a Repeat Calls (Student Concentrations) layer. The tabs included are [What?](#), [How?](#), [Where?](#) and [When?](#) The term Repeat Calls is used with CrimeView and FireView, while Student Concentrations is used in School Planner. School Planner does not support the When? tab, as all queries are expected to be made on the full year of student data.

What?

Attachment A

The What? tab is used to specify the following query parameters:

- **Query Layer**

Select the [Query Layer](#) from the list of point layers in the active data frame. The features in the Query Layer that satisfy both the attribute query and date or time range are used to generate the Repeat Calls (Student Concentrations) layer.

- Additional Query Layers

Select [additional layers](#) that can be included with the Repeat Calls (Student Concentrations) routine.

- Attribute Query

Once the [Query Layer](#) is selected, the saved query groups registered to the Query Layer are displayed in the [Saved Queries](#) tree or columns.

How?

The How? tab includes settings that control the way in which the Repeat Calls (Student Concentrations) layer is generated and displayed.

- New Layer Name

Enter the name for the new Repeat Calls (Student Concentrations) layer which is used when the layer is added to the active data frame's table of contents.

- Address Field

Select the field from the Query Layer that contains the address or location description. The values in this field are included in the resulting Repeat Calls (Student Concentrations) layer for reference only. The repeat calls (students) are determined spatially, consequently, it does not matter if the Address Field selected has different values in it, such as the different spelling of an address.

- Minimum Number

Enter the minimum number of features per location that are to be considered a repeat call (student concentration). The default value is 2 and the valid range is 1 to 5000.

- Top 10 Locations

Select the "Show only top 10 locations" checkbox if only the top 10 locations are to be displayed with the Repeat Calls (Student Concentrations) Layer.

Attachment A Show only Top 10 locations

- Options

There is one option available in controlling the look of the new Repeat Calls (Student Concentrations) layer.

Transparency

The transparency setting can also be used to ensure that points and lines below the new Repeat Calls (Student Concentrations) layer will not be obscured. Set the percentage of transparency for the new Repeat Calls (Student Concentrations) layer, where 0% means that the layer is opaque and 100% means that the layer is invisible. This transparency value can also be changed later by using the Display tab in the Layer Properties dialog. The default value is 20%.

Transparency: %

Where?

The Where? tab is used to select the boundaries used as the spatial query features when running the routine. The Where? tab is only enabled when the "Subset by boundary" checkbox is selected on the How? tab. There are two boundary types:

- Existing Boundary Layer

The features of an [existing boundary layer](#) are used to spatially query features. Select the boundary layer and then features to include in the spatial query.

When editing a [Cyclical Report](#) and the By Pointing selection method has been used, the features in the boundary layer will be selected.

- User Defined Area

The [User Defined Area](#) boundary type is a useful when there are no existing boundary layers that can be used to spatially query features.

When editing a [Cyclical Report](#) the user defined graphic element will be created on the active data frame and it is selected. To change the user defined boundary, delete the element and create a new one.

When?

Attachment A

The When? tab is used to specify a [date or time range](#). This tab is only available if the [Query Layer](#) set in the What? tab has OmegaGIS date and time fields. For School Planner, the When? tab is not available since queries are expected to be made on a full year of student data.

Running the Repeat Calls / Student Concentrations Routine

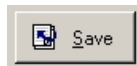
To create the Repeat Calls (Student Concentrations) layer, click the Finish button. The Finish button is only enabled when all of the parameters for the routine are set. The required parameters for the Hot Spot routine include:

- A [Query Layer](#) is set.
- When the "Subset by boundary" option has been selected and [existing boundary layer](#) is used at least one field value has been selected when the By Field Value selection method is used. When the By Pointing selection method is used, there is no check to ensure that features are selected in the boundary layer until the Finish button is clicked.

An attribute query and a date or time range are not required to run the Repeat Calls (Student Concentrations) routine.

When the Finish button is selected, the routine validates the parameters and then displays a summary dialog. The validation includes checking that there are features selected in the boundary when the By Pointing option is used when subsetting by boundary. When the boundary type of [User-Defined Area](#) is used, the graphic element is checked.

The summary dialog provides an overview of the parameters for the Repeat Calls (Student Concentrations) routine. Use the Back button to return to the query dialog to make edits to the routine. The Save button on the summary dialog allows the routine to be saved as a [Cyclical Report](#).



The "Display the routine summary dialog" option in the [OmegaGIS Setup](#) dialog controls whether the summary dialog is shown. The default option displays the summary dialog.

Results of Repeat Calls / Student Concentrations Routine

This section describes the results of the Repeat Calls (Student Concentrations in School Planner) routine and is divided into the

following topics:

[Results of Routine](#)

[RepeatCalls.MDB](#)

[Repeat Calls / Student Concentrations Layer](#)

Results of Routine

When the Repeat Calls (Student Concentrations) routine is successfully completed, the following events occur:

- The density dialog shrinks. To maximize the density dialog, double click the icon in the upper right corner. The [OmegaGIS Setup](#) dialog has a setting to hide rather than shrink the density dialog.
- The extent of the active data frame is changed to the extent of repeat call (student concentration) locations that are displayed plus a 5% buffer. If there is a spatial query, the active data frame zooms to the extent of the selected boundary features.
- The [Query Layer](#) and any [additional query layers](#) that are used to generate the Repeat Calls (Student Concentrations) layer have the following done to them:
 - Layer has visibility turned off.
 - The OmegaGIS [definition expression](#) is removed from the layer.
 - The selected features are cleared.
- If a boundary layer is used as a spatial query, the boundary layer has the following done:
 - The features used in the spatial query are selected. The "Select features used as boundaries..." option in the [OmegaGIS Setup](#) dialog controls this option.
 - The boundary layer is visible.
- If the [Repeat Calls Identify tool](#) is the active tool in ArcMap then Select Elements tool is made the active tool.

If no features are selected by the Repeat Calls (Student Concentrations) routine, the following events occur:

- The query dialog is maximized.
- A message box reports that the routine can not be completed. If [additional query layers](#) are used, the number on the message

Attachment A

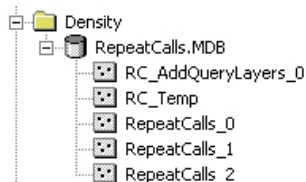
box reads 7810306 otherwise the number reads 7810439.

- The [Query Layer](#) and the additional query layers have their OmegaGIS [definition expression](#) removed.
- The visibility of the [Query Layer](#) reverts to its state before running the Repeat Calls (Student Concentrations) routine. If [additional query layers](#) were used all of the layers, including the Query Layer, will not be visible.
- The active data frame does not zoom.

RepeatCalls.MDB

During the running of the routine, a new feature class is generated in a personal Geodatabase. The Repeat Calls (Student Concentrations) layer is based on this feature class.

- The Geodatabase is named RepeatCalls.MDB and is located in the "Density" folder in the [project workspace](#).



- The RepeatCalls.MDB is created dynamically by the Repeat Calls (Student Concentrations) routine. If the Geodatabase is not present it will be created when the Repeat Calls (Student Concentrations) routine is run.
- When the routine runs, different feature classes are created in the RepeatCalls.MDB.

RepeatCalls_*

This feature class with the geometry type of multi-point is displayed in ArcMap as the Repeat Calls (Student Concentrations) layer. The "CNT_OmegaGIS_XY" field contains the count of the features at that location, this field name alias is "Incident_Count" in the Repeat Calls (Student Concentrations) layer. The "FIRST_ < Name of Address Field>" field contains the value from the Address field that is identified on the How? tab. The field name alias for this field is "Address" in the Repeat Calls (Student Concentrations) layer. The feature class is deleted when it is no longer referenced in the ArcMap document.

OBJECTID*	Shape*	Cnt_OmegaGIS_XY	Min_ADDRESS
4118	Multipoint	50	002635 N 63RD ST
861	Multipoint	42	000605 S 10 ST

Attachment A***RC_AddLayers_****

This feature class is created when [additional query layers](#) are used and contains all of the features from the different layers that are used when determining repeat calls (student concentrations). This feature class is used with the Repeat Calls (Student Concentrations) Report and the [Repeat Calls \(Student Concentrations\) Identify](#) tool. The RC_AddLayers_* feature class is only deleted when the "RepeatCalls_*" that was created from it is removed from the ArcMap document.

RC_Temp

This feature class is created when there is only one [Query Layer](#). This feature class contains all of the features to be used when determining repeat calls (student concentrations). The feature class is deleted during the [OmegaGIS Project Exit](#) and when a new Repeat Calls (Student Concentrations) routine is run.

Tip:

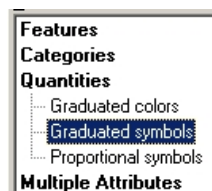
- To [permanently persist](#) the feature class created from a density routine, export the feature class to a different personal Geodatabase.

Repeat Calls / Student Concentrations Layer

The Repeat Calls (Student Concentrations) routine adds a layer to the active data frame whose data source is from a RepeatCalls_* feature class in the RepeatCalls.MDB. The Repeat Calls (Student Concentrations) layer has the following properties:

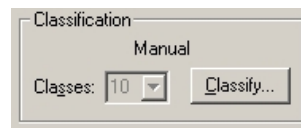
- ***Graduated Symbol***

The graduated symbol renderer is used with the Repeat Calls (Student Concentrations) layer. The size of the symbol changes based on the number of repeat calls (students) for the location.



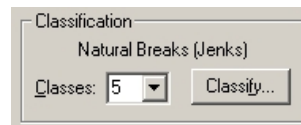
Top Ten

When the top ten locations are displayed, the legend will have ten class breaks. The manual classification is used to determine the class breaks. There could be more than ten features in the Repeat Calls (Student Concentrations) layer as two separate locations may have the same number of repeat calls (students). There may also be fewer than ten class breaks if there are less than ten unique repeat call (student) values based on the minimum number of features per location.

Attachment A

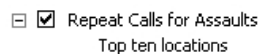
Display All Repeat Calls (Student Concentrations)

When the top ten locations are not being displayed but rather all of the locations that have repeat calls (students), the Jenk's Natural Breaks statistical formula is used to inspect the data and determine the class breaks. This method attempts to minimize the variance within the class and to maximize the variance between the classes. Five class breaks are used.



- Legend Heading

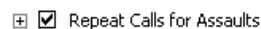
The legend heading will report "Top ten locations" when the top ten option was selected on the How? tab. If there were fewer than ten repeat call (repeat student) locations, the legend heading will be altered to state the number of repeat call (student) locations. The heading can be altered by double-clicking the text which makes the text editable.



There will be no legend heading if all of the repeat calls (student) locations are displayed.

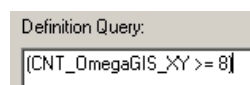
- Collapsed Legend

When there are more than five class breaks, the legend will be collapsed in the table of contents. To expand the legend click the plus icon to the left of the Repeat Calls (Student Concentrations) layer name.



- Definition Expression

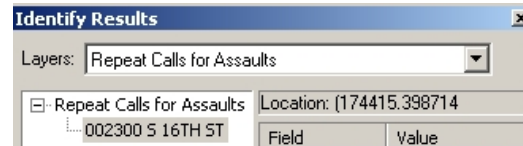
A definition expression limits the features that are displayed to those that satisfy an attribute query. The RepeatCalls_* feature class contains all of the locations that satisfied the attribute and spatial query and the definition expression is used to limit the Repeat Calls (Student Concentrations) layer to those locations that have a minimum number of features.



Attachment A

- Primary Display Field

The primary display field is used with the ArcMap Identify tool. The value of the field is shown on the right side of the Identify Results dialog rather than scrolling through the list of field values. The address field is set as the primary display field.



- Label

The address field is set to the label field of the Repeat Calls (Student Concentrations) layer.



Repeat Calls / Student Concentrations Identify Tool

Availability by Extension

CrimeView
Repeat Calls Identify

FireView
Repeat Calls Identify

School Planner
Student Concentrations Identify

The Repeat Calls / Student Concentrations Identify tool is used to retrieve information about the original features that made up a particular repeat call (student concentration) location. The tool is available when any OmegaGIS extension is enabled.

Active Repeat Calls / Student Concentrations Identify Tool

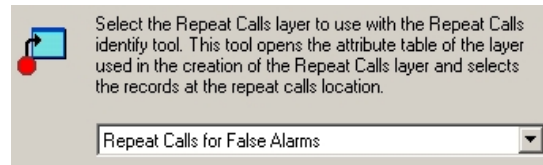
To make the Repeat Calls / Student Concentrations Identify tool active, select the tool from the CrimeView, FireView or School Planner toolbar.



If there are multiple Repeat Calls (Student Concentrations) layers in the active data frame, a dialog will open with a list of Repeat Calls (Student Concentrations) layers. Select the Repeat Calls (Student Concentrations) layer to select features from and select OK.

Attachment A

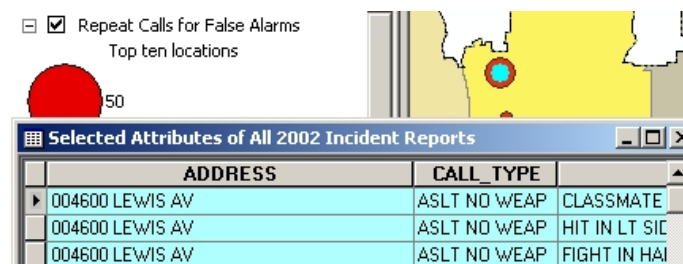
If there is only one Repeat Calls (Student Concentrations) layer, the tool will become active.



When the Repeat Calls / Student Concentrations Identify tool is active, the Repeat Calls (Student Concentrations) layer becomes visible. The mouse also changes to a pointer with a red letter "R" beside it when placed over the active data frame.

Identify Repeat Calls / Student Concentrations

To retrieve information about the original feature that made up the repeat calls (student concentrations), with the Repeat Calls / Student Concentrations Identify tool active, select the center of the repeat calls (student concentrations) location. The tool uses the ArcMap snapping tolerance for selecting locations. When a location is selected by the tool, an attribute table will open with the features that made up that repeat calls (student concentrations) location selected.



The original [Query Layer](#) must be in the active data frame and have the same name as when the Repeat Calls (Student Concentrations) layer was created for the identify to work. If the Query Layer cannot be found there is a message box (12505) and the Repeat Calls / Student Concentrations Identify tool will not longer be the active tool.

When [additional query layers](#) are used to create the Repeat Calls (Student Concentrations) layer, the RC_AddQueryLayers_* feature class in the [RepeatCalls.MDB](#) is used as the source of the original features.

Map Navigation

In ArcMap, only one tool may be active at any one time. Consequently, when the zoom or pan tools are used the Repeat Calls / Student Concentrations Identify tool will no longer be active. Below are two suggested map navigation options that keeps the Repeat Calls / Student Concentrations Identify tool active:

Attachment A

- Use the ArcMap Magnification dialog which is available from the Windows pull-down menu in ArcMap. The Repeat Calls / Student Concentrations Identify tool works inside of this window.
- Use the scroll bars on the active data frame to pan to different locations.

About Exception Reporting / Enrollment Comparison**Availability by Extension**

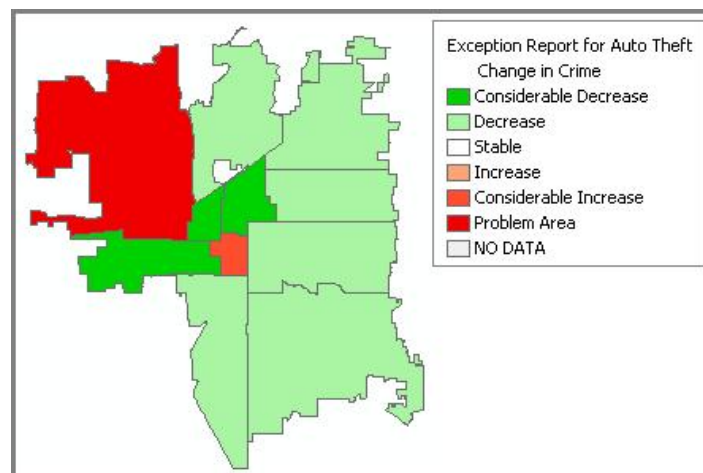
CrimeView	FireView	School Planner
Exception Reporting	Exception Reporting	Enrollment Comparison

Exception Reporting and Enrollment Comparison are based on the concept of comparing information from different periods in time in order to view trends in the data. Exception Reporting is available with CrimeView and FireView software products. In this case, Exception Reporting compares the number of incidents occurring over time in order to determine whether the area under observation has experienced stability, increasing or decreasing trends in activity.

Available with School Planner, Enrollment Comparison in the same way focuses on trends in the data, but in this case, examines the differences in student populations over time. Unlike Exception Reporting, Enrollment Comparison bases the analysis on the full year of student data. Exception Reporting has the functionality to select specific periods of time throughout the year.

Map Layer

The result of running an Exception Report or Enrollment Comparison is a new map layer that identifies the increase, decrease or stability of the data by geographic boundary.



Attachment A

To calculate the change in the number of incidents (or students) that have occurred over time, there must be a historical record of the incidents (students) in question. If no incidents (students) are found in the previous layer based on the query run with the analysis, the percent change cannot be calculated. The change in the number of incidents (or students) is calculated as:

$$(\text{Current Data} / \text{Previous Data} - 1) * 100$$

As this equation is not divisible by zero, the data count from the historic layer must be included in the calculation to proceed. In cases where the count for previous incidents or students for an area is zero, the percent change is given a value of No Data.

Map Legend

The change in incidents (students) over time is identified by classifying the increase or decrease into different thresholds of percent change. Based on the analysis run, these classifications vary due to the fact that the change in students over time is usually on a much smaller scale than that found for incidents of crime or fire.

The divisions for Exception Reporting are as follows:

<i>Legend Value</i>	<i>Legend Description</i>
-100 to -50	Considerable Decrease
-50 to -10	Decrease
-10 to +10	Stable
+10 to +50	Increase
+50 to +100	Considerable Increase
100 to 10000	Problem Area
NO DATA	No crimes occurred initially

The divisions for Enrollment Comparison are as follows:

<i>Legend Value</i>	<i>Legend Description</i>
-6 to -3	Considerable Decrease
-3 to -1	Decrease
-1 to +1	Stable
+1 to +3	Increase
+3 to +6	Considerable Increase
6 to 100	Problem Area
NO DATA	No historic students found

Map Results

Attachment A

When an Exception Report or Enrollment Comparison is run, a new layer is generated and placed in the ArcMap table of contents. The new layer is based on the total number of incidents (or students) involved in the query. As there is a 10,000 percent increase cap on the incident data (100 percent increase in the case of students), those areas exceeding this value will not show up in the new layer. To view these areas, open the properties dialog of the layer, and increase the upper limit of the 'Problem Area' to the maximum found in the new layer.

Report Results

In addition to the new layer created by the analysis, a Crystal Report is generated. The report is based on a template that is provided with the software installation, and can be found in the \reports folder. The format of this report can be modified however, the data should not be altered as it is based on the standardized output of the Exception Reporting / Enrollment Comparison analysis.

Lincoln Police Department				
Exception Report				
April 14, 2003				
Auto Theft - January to March				
REPORT AREA	PREVIOUS	CURRENT	DIFFERENCE	PERCENT
ABBAULT				
1A	40	65	25	62.50%
1B	30	50	20	66.67%
2A	49	53	15	34.69%
2B	19	102	23	92.11%
4A	34	59	19	55.88%
4B	57	43	-9	-15.79%
4C	39	30	-9	-23.08%
5A	39	40	1	2.56%
5B	31	29	-2	-6.45%
7A	30	41	11	36.67%
7B	11	63	9	4.23%
Total	437	628	192	20.84%
AUTO THEFT				
1A	4	14	10	250.00%
1B	3	5	-9	-30.00%
2A	9	5	-4	-44.44%
2B	10	3	-2	-20.00%
4A	14	7	-7	-50.00%
4B	7	11	4	57.14%
4C	9	9	-2	-40.00%
5A	5	4	-1	-20.00%
5B	5	9	-2	-40.00%
7A	4	2	-2	-50.00%
7B	21	10	-11	-52.38%
Total	82	72	-20	-21.74%

Exception Reporting / Enrollment Comparison Setup

Exception reporting (Enrollment Comparison) is a comparison between historical and current data. The routine enables the identification of changes in the data within a geographic area. In order for layers to become available to the Exception Reporting (Enrollment Comparison) routine there are several options that should be set prior to using the utility.

[Setting Up Layers](#)

[Saved Queries](#)

[Reporting](#)

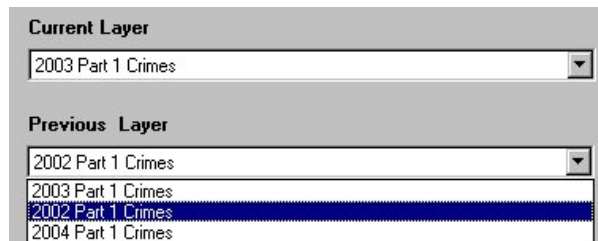
[Field Schema](#)

[Maximizing Performance](#)

Setting up Layers

Current Layers

Two layer lists exist on the What? tab (Current Layers and Previous Layers) that provide the basis for comparing historic to more current data. By selecting a Current Layer, the Previous Layer list box is populated with layers that meet specific requirements based on the Current Layer selected.



The Current Layer in the analysis, represents the layer that is compared to historical events in order to determine changes that have occurred over time. To appear in the list, the Current Layer must have a geometry type of point. Multipoint layers are not supported. The data source of the layer must be valid. If the data source is invalid, a red exclamation mark appears at the left hand side of the layer name in the map table of contents.

2003 Part 1 Crimes

Selection layers are not included in the layer list. Selection layers are created as a result of running OmegaGIS routines. Selection layers share the same data as the layer on which they were based during the query. Consequently, including these layers in the layer list, essentially results in displaying duplicate data.

Often a project can become confusing when many different layers exist within the map from which to query. To narrow down the list of layers that may be displayed in the layer list, two options can be set using [Setup](#). The first option deals with the use of registered layers. As layers are created, they can be registered as different types using the [OmegaGIS Metadata Editor](#) in ArcCatalog . Once registered, the setting 'Only use registered layers to create new queries' within the Queries category in [Setup](#) can be toggled to display only those layers registered as a specific type.

To limit the layer list further, those layers created by OmegaGIS routines may be excluded from the list explicitly using the 'Exclude layers...' checkbox on the Advanced tab of the Queries category. Setting this option ensures that layers created by any of the OmegaGIS routines cannot be selected.

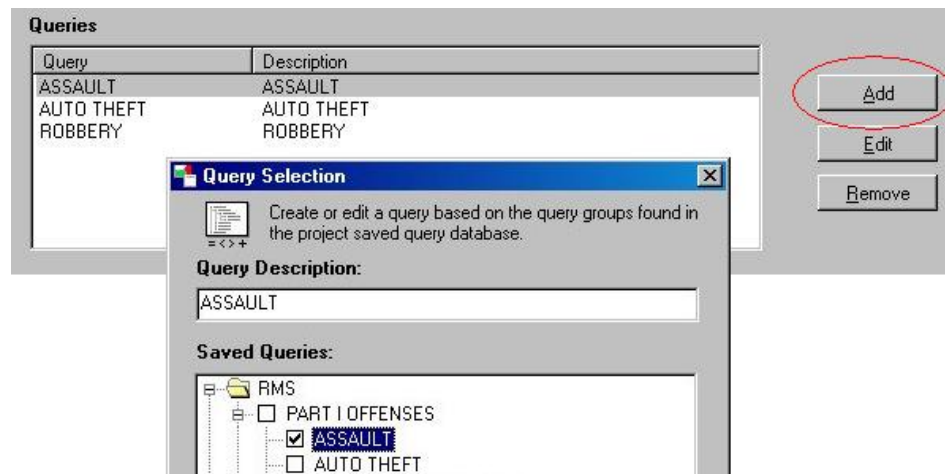
Previous Layers

Previous Query Layers are point layers used as the historical comparison to the Current Layer. The list is populated based on the Current Layer selected. The Current Layer is included in the list so that comparisons can be made using date ranges within the same layer. Previous Layers are only available to those Current Layers that share the same Query Groups and field list. However, they may include additional fields not found in the Current Layer.

Attachment A**Saved Queries**

The [Saved Queries](#) database (Omega_Query.odb) is an extremely important component of any OmegaGIS project. The database stores common queries that will be used frequently to query the available datasets . This database is usually compiled at the beginning of a project, in a combined effort between the Omega Project Manager and the Client. Queries that will be used frequently to analyze data are identified and added to the database using the [Omega Query Editor](#) so that they may be accessed from OmegaGIS routines.

Most OmegaGIS routines display saved queries within a Saved Queries Tree or Column view on the **What?** tab of the dialog. Exception Reporting (Enrollment Comparison) is slightly different in that the Saved Query Tree or Column view is accessed through the 'Add' button on the **What?** tab. As each Saved Query is added to the active project, the name of the saved query is added to the 'Queries' list on the What? tab.



Since the Current and Previous Layers must share the same Query Groups if they are to be compared, the Query Groups must be registered to both layers. A Query Group is simply a container for all of the related queries collected within it. The Query Group can be recognized as the root folder(s) in the Saved Query Tree. The [OmegaGIS Metadata Editor](#) can be used to register the Query Groups to the appropriate layers.

Reporting

The Exception Report is a Crystal Report that has been customized to work with the Exception Reporting routine. A template for this report can be found in the <installation folder>\OmegaGroup\Desktop\Reports folder called Exception.rpt. The report can be modified in format and fields in order to display additional information. The original fields however, should not be altered as they are based on standardized data output from the routine.

When the report has been customized, it can be placed in any folder, as long as the path to that folder is referenced in the Locations Category for Crystal Reports in Setup. The report name should not be changed however, as it is searched for by name in the Exception Reporting routine.

Field Schema

A field schema refers to the fields that make up a layer's dataset. Each field is defined by field characteristics such as a field name, data type, precision etc. In order to compare Current and Previous layers, the Current Layer must contain all of the fields contained within the Previous Layer, as well as retain the same field characteristics as that of the Previous Layer.

-

Maximizing Performance

-

Sample Rate

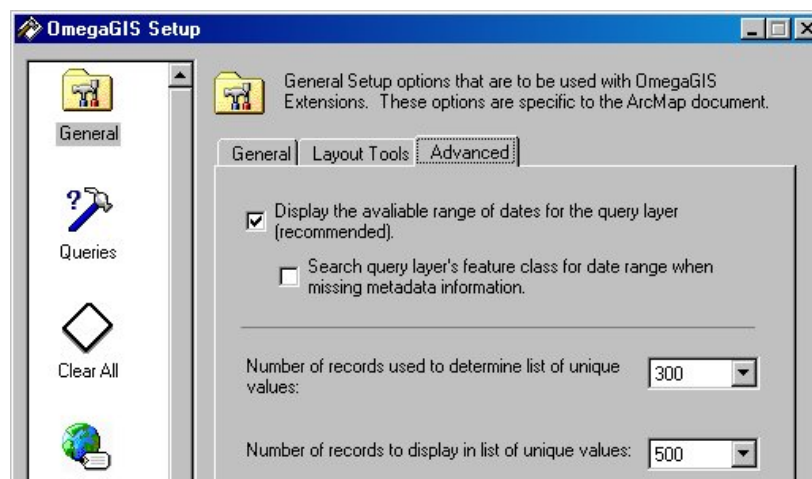
The exception report (enrollment comparison) and map generated by the analysis, may be limited to specific geographic regions by selecting polygon field values available on the dialog. When using layers with a large number of geographic boundaries, the field value list may become quite long and difficult to update and navigate, and thereby impede performance. To assist in performance, a sample rate can be set to limit the number of polygons that are used to create the unique field values list. The sample rate is accessed through [Setup](#).

-

-

Maximum Unique Values

The maximum unique values setting in [Setup](#) is also useful in gaining performance when dealing with layers with many boundaries. The maximum unique values setting identifies the maximum number of unique field values that may be displayed in the field value drop-down list. If the maximum number is hit, a warning message is displayed next to the list to indicate that not all values are displayed.



Exception Reporting / Enrollment Comparison Menus

Attachment A

The Exception Reporting and Enrollment Comparison Menus are identical with the exception of the When? tab. The When? tab is absent from the Enrollment Comparison analysis, as student population comparisons are always created on the entire student year. The following sections identify the What?, Where? and When? tabs, and describe the choices that are available on each.

[What?](#)

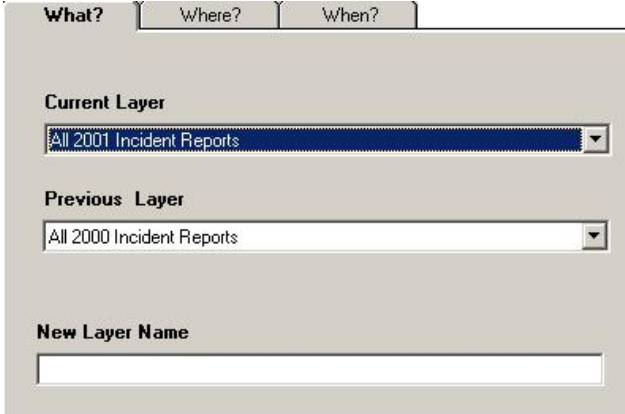
[Where?](#)

[When?](#)

What

The **What?** tab includes the ability to select from available current and historic data layers of interest. Previous layers (or historic layers) are included in the dropdown list based on the layer selected from the Current Layer list box. For a description of the way in which the Previous layers are updated, read the [Reporting Setup](#) section.

Below these layer choices, the New Layer Name textbox can be used to enter a name that will appear in the ArcMap table of contents once the analysis is complete and the map layer has been added to the active view.

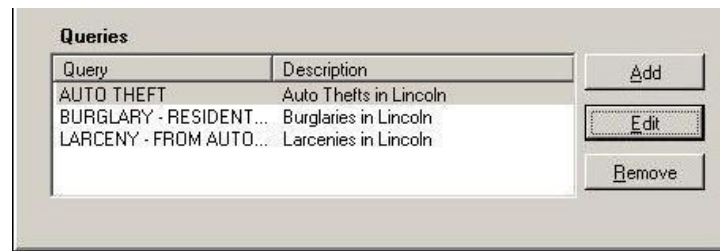


The screenshot shows a software interface with three tabs: 'What?', 'Where?', and 'When?'. The 'What?' tab is active. Below the tabs, there are three sections:

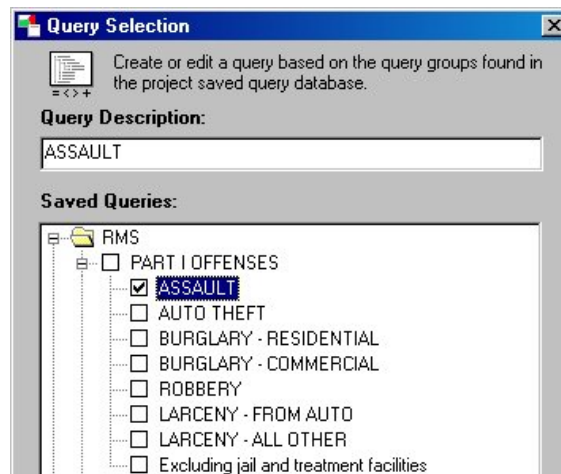
- Current Layer:** A dropdown menu with 'All 2001 Incident Reports' selected.
- Previous Layer:** A dropdown menu with 'All 2000 Incident Reports' selected.
- New Layer Name:** An empty text input field.

Queries

Queries are created by accessing Saved Queries available to the Previous and Current layers. A query may be added, edited or removed from an Exception Report (Enrollment Comparison) analysis. Each query represents a category that may be viewed by the Exception Report (Enrollment Comparison) Viewer. On completion of an Exception Reporting (Enrollment Comparison) routine, the initial map and report generated are based on the total number of data points selected using all of the queries in the list.

Attachment A**Query Selection**

Queries may be composed of one or more saved queries. Saved queries are created during the installation of the project, and are stored in one or more Saved Queries databases. The syntax of the Saved queries may not be edited within the Exception Reporting (Enrollment Comparison) analysis menu, however, queries, which are the combination of the saved queries may be modified or updated.

**Where**

The **Where?** tab controls from which geographic boundaries the data points are selected to complete the analysis. A boundary layer is selected from a list available on the dialog. To narrow down the analysis to a specific geographic region, individual boundaries within the layer may be selected by choosing a field value on the menu, or by interactively pointing to boundaries on the map.

Attachment A

The screenshot shows a dialog box with three tabs: 'What?', 'Where?' (selected), and 'When?'. The 'Where?' tab contains the following elements:

- Boundary layer:** A dropdown menu currently showing 'Neighborhood Association'.
- Selection Method:** Two radio buttons. 'By Field Value' is selected, and 'By Pointing' is unselected.
- Field Value Selection:** A 'Field name' dropdown menu set to 'NAME', and a list box showing three items: 'Highlands', 'Bicentennial Estates', and 'West Lincoln'.

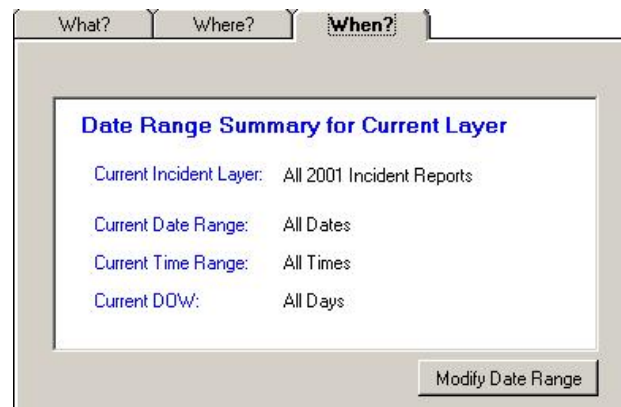
Performance

Two settings are available in [Setup](#) that boost performance when populating the field value list box. These settings influence performance by limiting the number of unique values displayed. They are important when using very large data sets, where populating the list box may impede performance.

The sample rate setting identifies how many features will be used to retrieve unique field values from the boundary layer. The maximum unique value option determines the number of unique values that can be displayed in the list box. The Complete List button below the field values list box on the dialog can be used to sample all of the features in the layer to create the unique values list. If the maximum number of unique values exceeds the limit set in [Setup](#), a warning message appears on the dialog, indicating that all field values are not displayed.

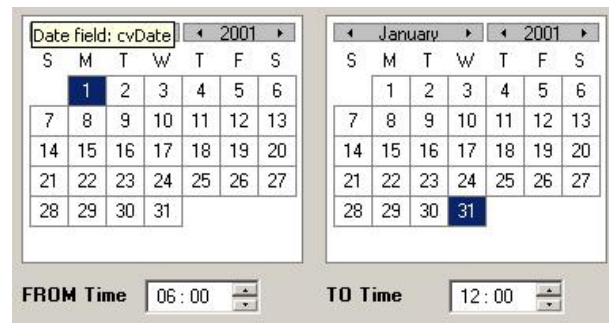
When

The **When?** tab displays a summary of date and time range information for both the Previous and Current layers. To change the date settings for either of these layers, use the 'Modify Date Range' buttons to open a DateTime dialog. Remember that this tab is only available with Exception Reporting in CrimeView and FireView as Enrollment Comparisons are always performed on a full year of student data in School Planner.

Attachment A**From Date & To Date**

The From and To Date calendars set the date range from which incidents are selected for the analysis. Dates falling outside the available date range are colored grey.

Hovering over the From Date or To Date text displays the date field on which the calendars are based. If multiple OmegaGIS Date fields exist in the layer, the Options button may be used to modify the date used by the calendars.

**From Time & To Time**

From Time and To Time are available to limit the incidents included in the routine to a specific range.

Note: A date and time range of March 1st to March 5th from 1:00pm to 6:00pm indicates that incidents from the 1st to the 5th of March that occurred between the hours of 1 and 6 pm will be included in the analysis.

Previous Range

The Previous Range is available in order to select a date duration. Select the number of hours, days, weeks, months or years

Attachment A

from the drop-down lists available, and the From and To Date calendars are set automatically.

* It is important to note that the duration represents the last complete block of dates. For instance, given that the current date is December 9th, a previous duration of 1 month returns the dates between November 1st and November 30th. The dates between December 1st and the 9th are excluded as they are not a part of a complete month.

Predefined Date Range & Predefined Time Range

Four predefined date ranges are available for use which include Today, Week To Date, Month To Date and Year To Date. Predefined time ranges include Day (6am to 6pm) and Night (6pm to 6am). Additional date and time ranges may be created using the Organize button on the dialog. Date and time ranges can be entered and are saved to the Settings.MDB so that they may be used again in future analyses.

Name	Range
Jan	3/1/2000 - 3/22/2000
Feb	3/1/2000 - 3/22/2000

New date range:
1/1/2000 - 1/31/2000

Day of Week

If a Day of Week field is available in the data, incidents included in the analysis may be limited to specific days of the week.

Options

The fields on which date and time ranges are based may be selected using the Options button. To change the default date and time fields permanently, use the OmegaGIS Metadata Editor <LINK> available within the OmegaGIS Data Manager extension in ArcCatalog.

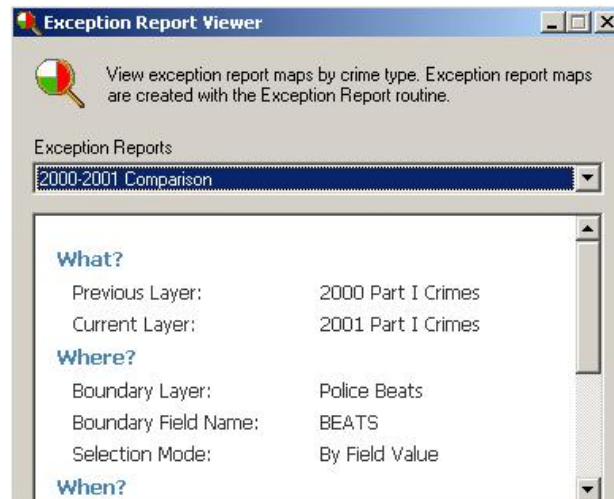
Exception Report Viewer / Enrollment Comparison Viewer

The Exception Report Viewer, also known as the Enrollment Comparison Viewer in School Planner, displays the results of

Attachment A

[Exception Reporting](#) (Enrollment Comparison). When an analysis is run using one of these routines, it is possible to create multiple queries that display different aspects of the data.

For example, in Exception Reporting, several queries might be included to reveal different incident types that have occurred. In the case of Enrollment Comparison, queries may be designed to view the number of students enrolled in different grades. When the Exception Report (Enrollment Comparison) results are generated, the results are based on the total number of incidents or students generated by all of the queries. The Viewer tool creates the ability to view the individual queries involved in the analysis.



On opening the Viewer, a list of available reports that have been generated by the Exception Report / Enrollment Comparison tool is displayed in the Reports list box. After selecting a report to view, metadata describing the report, and a list of queries that were used in generating the report is populated.

After selecting a query, and entering a name for the new layer that will be generated, clicking 'Finish' creates the new map layer. The transparency and placement of the new layer in the ArcMap table of contents can be modified using the Advanced button.



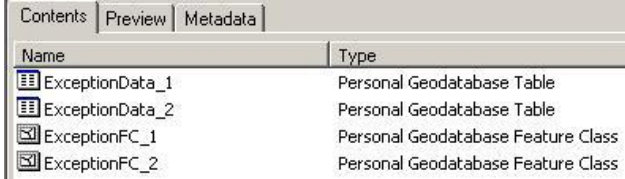
Attachment A

In addition to creating a map, a report can be generated by clicking on the 'View Report' checkbox. The report summarizes the data for each query used in the routine. In order to display the report, the report template called Exception.rpt MUST be located in the project's \reports folder.

Exception Report Data

Exception Report data is stored within the ExceptionData.MDB geodatabase located in the [Project Workspace](#) \Analyses folder. The feature classes and tables stored within the geodatabase are automatically deleted when the project is closed, as long as they are not found in the map table of contents. In order to manually delete a layer from the Exception Reports list box on the dialog, the layer must be removed from the geodatabase.

Within the geodatabase, the data associated with the exception reporting layer is divided into a feature class and a table. The link between the feature class and table can be identified by the number within the filename. To identify the report name found in the exception report view list box, the metadata tag /theomegagroup/exceptionreporting/reportname can be viewed from the metadata tab in ArcCatalog.



Name	Type
ExceptionData_1	Personal Geodatabase Table
ExceptionData_2	Personal Geodatabase Table
ExceptionFC_1	Personal Geodatabase Feature Class
ExceptionFC_2	Personal Geodatabase Feature Class

Deleting Exception Reporting Data

In general it is not a good idea to manually remove the exception reporting data from the geodatabase. Deleting the unused feature classes and associated tables from the geodatabase can be accomplished using [Setup](#). In the General category, click the 'Apply Project Cleanup' on the General Tab. The 'Apply Project Cleanup' button removes any OmegaGIS files that are not currently used in the project. Consequently, it clears the ExceptionData.mdb of all unused files when applied.

About Crime Rate Generator / Demographic Analysis

Crime Rate Generator and Demographic Analysis are very similar in design and in how they process data to create statistical results. Crime Rate Generator is available with CrimeView while Demographic Analysis is accessible using School Planner. Due to the similarity in the nature of their design, they are both described below. Where there is variation in the parameters required by the routine, or the results generated, these items are identified.

Availability by Extension

CrimeView	FireView	School Planner
Crime Rate Generator	Not Available	Demographic Analysis

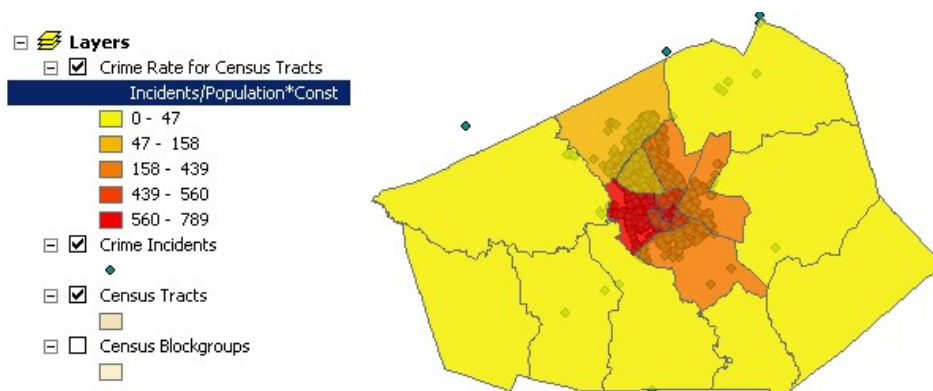
Crime Rate Generator

Crime rates are used to tie demographic characteristics to crime data. Crime Rate Generator provides an easy method for creating thematic maps used to view and analyze crime rates. Crime rates are calculated by dividing the number of incidents within a given boundary by the population count. The equation used in calculating crime rates is defined below:

$$\text{Crime Rate} = (\text{Incidents} / \text{Population}) * \text{Constant}$$

The constant in the above equation may vary between 100 and 100,000, and is used to create meaningful crime rate statistics dependent on the size of the population. For instance in a town of 8,000, with the number of crime incidents totaling 500, using a constant of 1,000 results in a crime rate of 62.5 crimes per 1,000 people. A constant of 100,000 (crimes per 100,000 persons) is typically used to compare crime rates for much larger areas such as between states or countries.

Crime rate results are displayed in a thematic map, which is added to the data frame of the current ArcGIS project.



Crime Rate Generator is available from ArcMap when both incident and census layers can be found within the active data frame.

Considerations in calculating crime rate statistics begin with ensuring that comparative analyses use similar durations. For instance, a crime rate calculation based on a yearly sampling of data, is not suitable for a comparison of monthly data. In addition, when looking at different neighborhood types, crime rates may appear unusually high. For instance, a commercially zoned neighborhood may indicate abnormally high crime rates, due to a low residential population. An understanding of the spatial and temporal information used in any analysis is important when attempting to produce meaningful results.

Crime Rate Generator Results

Attachment A

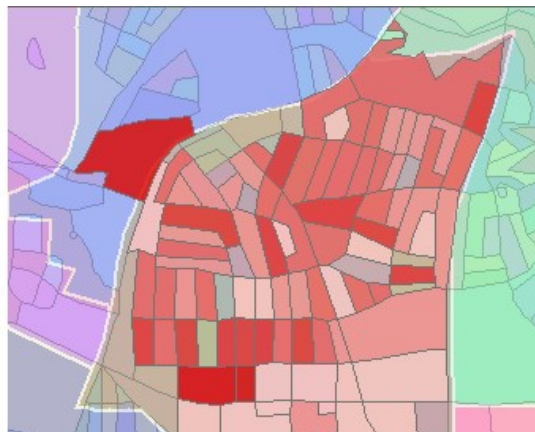
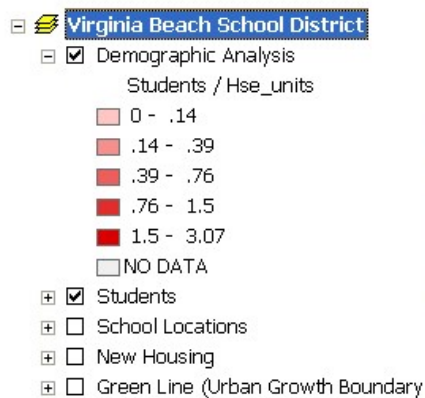
The result of a Crime Rate Generator routine is a new layer and report that identify the crime rate statistics for geographic regions. The new Crime Rate layer is displayed on the map, while the data source of the layer is stored in a database called CrimeRateData.mdb in the project \Census folder. When the ArcMap project is closed, any crime rate layers that are not saved in the map table of contents are deleted automatically from the database.

Running the Crime Rate Generator Routine

In order to run Crime Rate Generator, layers with point type geometry must exist in the table of contents. These layers should contain the incident data used in the analysis. In addition, census layers must exist in the map table of contents and are identified using metadata tags associated with the layer. These tags are generated automatically when the Omega Demographic Data Loader is used to create the data. However, the OmegaGIS Metadata Editor may also be used to register the layers as census layers. Once census layers are created, they may be stored as shapefiles, in a personal geodatabase or as ArcSDE layers.

Demographic Analysis

Demographic Analysis is an excellent tool for calculating student generation rates based on school zones. A student layer is selected, and then compared against the number of housing units found in a particular school zone. In addition, this tool can be used to generate population statistics to compare the number of students queried with census data available for any block, blockgroup or tract in the school district.

**Demographic Analysis Results**

The result of a Demographic Analysis is a new map layer and report that identify either the student generation rates for a particular school zone, or student statistics compared against the available census data. The new Demographic Analysis layer is displayed on the map, while the data source of the layer is stored in a personal geodatabase called StudentData.mdb in the project \Census folder. When the ArcMap project is closed, any layers generated by this analysis that have not been saved with the project, will be removed automatically from the map, and deleted from the source database.

Attachment A**Running the Demographic Analysis Routine**

To run a Demographic Analysis, layers with point type geometry representing the students for each school year must exist in the table of contents. In addition, census layers must exist in the table of contents. Census layers are identified using metadata tags associated with the layer. The tags are generated automatically when the Omega Demographic Data Loader in ArcCatalog is used to create the data. However, the OmegaGIS Metadata Editor may also be used to register the layers and set the appropriate metadata tags. Once census layers are created, they may be stored as shapefiles, in a personal geodatabase or as ArcSDE layers.

Crime Rate Generator / Demographic Analysis Setup

Both Crime Rate Generator and Demographic Analysis are designed to provide an easy method for comparing incident or student data found within geographic boundaries to census data available for the region. These tools were designed to use census data downloaded from the [ESRI](#) website as the demographic component, however, it is possible to use other sources of census information provided the data conforms to the requirements set by the routines. The following sections outline the work flow for creating meaningful statistical results using these analytical tools.

[Assemble the Census Personal Geodatabase](#)

[Create Saved Queries](#)

[Register Query Groups to Layers](#)

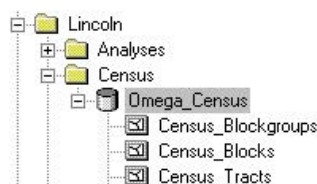
[Set Table of Contents](#)

Assemble the Census Personal Geodatabase

Crime Rate Generator and Demographic Analysis use census data to produce statistical results. In other OmegaGIS routines that provide the option to select areas geographically, any polygon layer found in the table of contents is available to delineate the spatial extent of the query. These two routines however, are based solely on census boundary layers. Census tracts, block groups and blocks are the only boundaries that may be used to calculate statistics.

Census data is available on the ESRI website, and once downloaded can be compiled using the OmegaGIS Demographic Data Loader. This utility is available on the Omega Data Manager extension in ArcCatalog. For a description of how to obtain the data as well as create the census boundary layers, read the information pertaining to the OmegaGIS [Demographic Data Loader](#). In using sources of census information outside of ESRI, the data must be provided as a shapefile, personal geodatabase feature class or ArcSDE layer. Each census layer must be registered using the OmegaGIS [Metadata Editor](#) with a layer type of 'Census_Tract', 'Census_Blockgroup' or 'Census_Block'.

Accessing Crime Rate Generator or Demographic Analysis requires that the census data adhere to the rules mentioned above. If the data does not exist in this format, a warning is issued when trying to open the routine dialog. The OmegaGIS Demographic Data Loader provided, formats the data automatically so that it is ready for these routines.



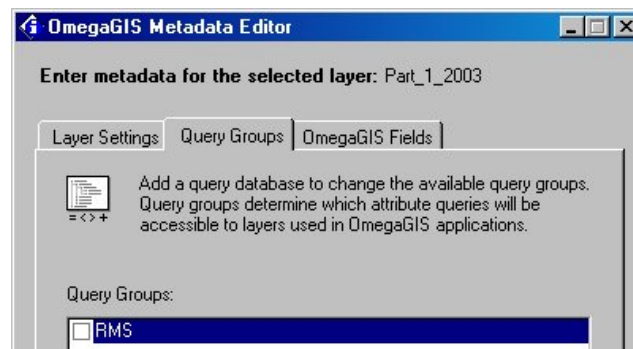
Attachment A**Create Saved Queries**

Saved Queries are essentially stored queries that can be accessed by OmegaGIS routines, including Crime Rate Generator and Demographic Analysis. When designing a project, the queries that will be used frequently on the data are identified, and saved. Each Saved Query provides an intuitive description to the user on the dialog, while behind the scenes storing the SQL syntax required by the source database. Saved Queries may be displayed as a tree view or alternatively in a column view. These options are available using OmegaGIS Setup.

For detailed information on this topic see [Saved Queries](#).

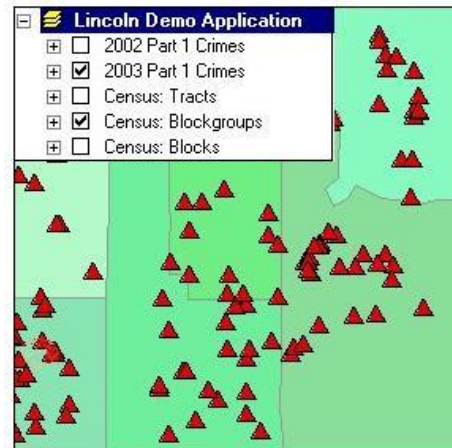
**Register Query Groups to Layers**

Query Groups must be linked to the appropriate layers in order to display the Saved Queries contained within the Group on the dialog. Before Crime Rate Generator or Demographic Analysis will display the Query Groups related to the layer, they must be registered using the OmegaGIS [Metadata Editor](#). The Metadata Editor is provided as a component of the Omega Data Manager extension in ArcCatalog. Once registered, these routines have access to any of the Saved Queries found within the registered Query Group.

**Set Table of Contents**

Attachment A

The last stage in accessing Crime Rate Generator or Demographic Analysis is to ensure that the data required for querying crime statistics or student statistics and the census data is located within the table of contents in ArcMap . If either the crime/student data or the census boundary layer information is missing, a warning message is issued that Crime Rate Generator or Demographic Analysis is unavailable.



Crime Rate Generator / Demographic Analysis Menus

Three tabs, **What?**, **How?**, **Where?** contain the options and settings necessary for calculating and displaying the results of Crime Rate Generator or Demographic Analysis. A fourth tab **When?** is available to Crime Rate Generator only. The questions that must be answered in order to fill in the parameters of the analysis include: Which incidents or students are to be selected for the analysis? How are the results to be displayed on the map? From which geographic areas are the incidents or students to be selected? and for Crime Rate Generator; Within what time frame should the incidents have occurred?

[What? Tab](#)

[How? Tab](#)

[Where? Tab](#)

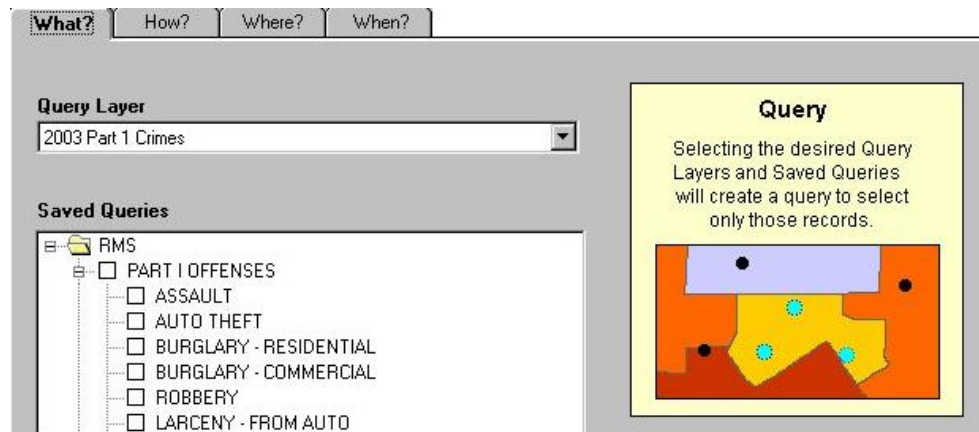
[When? Tab](#)

What?

The settings on the **What?** tab are used to identify the incidents or students of interest. A layer must be picked from the Query Layer list. The incidents or students may be narrowed down further by selecting a query from the [Saved Queries Tree](#) (or saved Queries Columns). Only those features matching the criteria of the saved query are used in generating the statistics. A saved query may also be modified using the 'Edit Query' button on the dialog.

Attachment A

In order for layers to show up in the Query Layer list, the data source must be valid, and the layer must have a geometry type of point. Additionally, if the 'Use registered type...' setting is checked in [OmegaGIS Setup](#), then only those registered types selected will be shown in the layer list.

**How?****Statistics**

The **How?** tab includes settings that control the way in which the map is displayed, as well how the statistics are calculated. The Census boundary layers are used to geographically group data for statistical calculations. The population field identifies the attribute within the census layer that will be used to calculate statistics.

Census Layer
Census: Tracts
Population Field
Pop2000

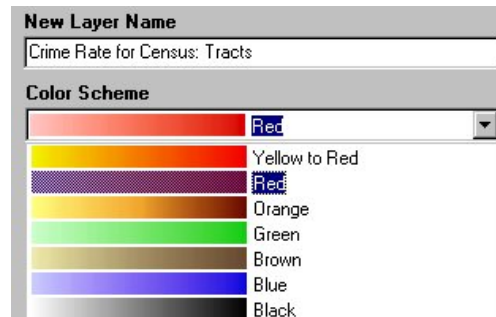
With Crime Rate Generator, calculating crime rates is accomplished using the following equation: Crime Rate = Incidents / Population) * Constant

With Demographic Analysis, the same calculation can be used (Students / Population) however, in this case the option for the constant is not necessary, and it is not available on the dialog. In addition to comparing student populations to general populations, using housing units in the equation allows for the calculation of Student Generation Rates. A Student Generation Rate is calculated by selecting the housing unit field available in the census data instead of the population field; so that the equation becomes (Students / Housing Units).

Attachment A**Layer Display**

Several settings are available to modify the look of the new layer. The color ramp provides several color options for displaying the resultant data. Color ramps are found in the [OmegaGIS.STYLE](#) file.

The name of the layer can be edited in the 'New Layer Name' text box.

**Options****Show Below Point and Line Layers**

Use the Show Below Point and Line Layers checkbox to have the new layer placed below all layers that have point and line geometry in the active data frame. By default, the new layer is added at the top of the table of contents and may obscure point or line layers below it.

Show Report

Each census layer (tracts, blockgroups or blocks) has a report template that is provided within the Omega Desktop installation folder. These reports can be found within the \omegagroup\desktop\reports folder, and can be customized and placed anywhere on disk. If the reports are placed in a location other than the project workspace's \report folder, the location must be identified in Omega Setup within the Locations category for reports.

Attachment A**Population Constant (available with Crime Rate Generator only)**

The constant in the crime rate equation may vary between 100 and 100,000, and is used to create meaningful crime rate statistics dependent on the size of the population. For instance in a town of 8,000, with the number of crime incidents totaling 500, using a constant of 1,000 results in a crime rate of 62.5 crimes per 1,000 people. A constant of 100,000 (crimes per 100,000 persons) is typically used to compare crime rates for much larger areas such as between states or counties.

Transparency

Transparency can be set to prevent the new layer from obscuring features in the layers below. Default values fall between 0 and 100, where 100 results in an invisible layer, and 0 is opaque. The default value is set at 20, allowing features below the new layer to remain visible. The transparency of the new layer may also be altered by using the Display tab in the Layer Properties dialog.

Where?

The **Where?** tab provides options to narrow down the number of polygons selected from the census layer on which to perform the calculations. Polygons may be selected by using the unique field values found in the layer or, alternatively, by pointing to the polygons on screen. Limiting the number of polygons involved in the statistical calculations improves the overall performance of the query.

The screenshot shows a software interface with four tabs: 'What?', 'How?', 'Where?' (selected), and 'When?'. The 'Where?' tab contains two main sections:

- Selection Method:** Two radio buttons are present: 'Field Value' (selected) and 'Pointing' (unselected). There is a small button with three dots next to 'Pointing'.
- Field Values:** A 'Field Name' dropdown menu is set to 'Pop2000'. Below it, a list box shows the following values: 3745, 4604, 4376, and 3695. The value 4376 is highlighted in blue.

To the right of these sections is a 'Boundary' panel with a yellow background. It contains the text: 'The boundary is used to select the points that will be included in the crime rate calculation.' Below the text is a small map showing a yellow boundary on a red background, with several black dots representing points. Some points are inside the boundary, and some are outside.

Field Value

Attachment A

To use the Field Value selection method, click on the Field Value radio button, then select from a list of field names in the Field Name list. Once a field name is selected, the field values available are updated and can be selected.

Complete List

The Complete List button at the bottom of the field values list box controls the number of field values that are added to the list. Within OmegaGIS Setup there are two important settings that control the field values list box. On the Advanced Tab of the General Settings category, the 'Number of Records used...' setting controls the number of polygons that are sampled in the boundary layer to get the unique list of values. The 'Number of records to display...' setting identifies how many of these unique values are displayed in the field values list. The complete list button ensures that all polygons in the boundary layer are sampled. If the number of unique values exceeds the value of the setting in Setup, a warning is displayed beside the list box.

By Pointing

The By Pointing method of polygon selection provides a means to selecting boundaries geographically. Click on the By Pointing radio button, then click the ellipses button (...). The routine dialog shrinks, and pauses while polygons are selected. When finished, click on the flashing icon in the top right corner to maximize the dialog.

When? (only available with Crime Rate Generator)

The **When?** tab displays a Date-Time dialog that can be used to select data from a specific date range. The dialog is common to most OmegaGIS routines. This tab is excluded from the Demographic Analysis routine as student statistics should be generated on the student data for the entire year.

From Date & To Date

The From and To Date calendars set the date range from which incidents are selected for the analysis. Dates falling outside the available date range are colored gray.

Hovering over the From Date or To Date text displays the date field on which the calendars are based. If multiple OmegaGIS Date fields exist in the layer, the Options button may be used to modify the date used by the calendars.

Attachment A

The screenshot shows two date selection calendars side-by-side. The left calendar is for the year 2001, with the month of January selected. The right calendar is also for 2001, with the month of January selected. Below the calendars are two time selection fields: 'FROM Time' set to 06:00 and 'TO Time' set to 12:00. The 'FROM Time' field has a dropdown arrow, and the 'TO Time' field has a dropdown arrow.

From Time & To Time

From Time and To Time are available to limit the incidents included in the routine to a specific range.

Note: A date and time range of March 1st to March 5th from 1:00pm to 6:00pm indicates that crimes from the 1st to the 5th of March that occurred between the hours of 1 and 6 pm will be included in the analysis.

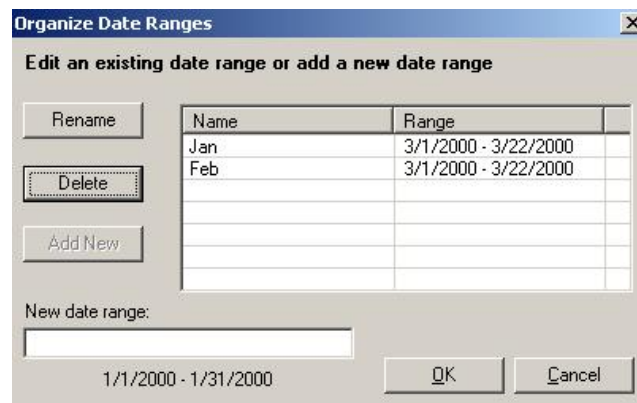
Previous Range

The Previous Range is available in order to select a date duration. Select the number of hours, days, weeks, months or years from the drop-down lists available, and the From and To Date calendars are set automatically.

* It is important to note that the duration represents the last complete block of dates. For instance, given that the current date is December 9th, a previous duration of 1 month returns the dates between November 1st and November 30th. The dates between December 1st and the 9th are excluded as they are not a part of a complete month.

Predefined Date Range & Predefined Time Range

Four predefined date ranges are available for use which include Today, Week To Date, Month To Date and Year To Date. Predefined time ranges include Day (6am to 6pm) and Night (6pm to 6am). Additional date and time ranges may be created using the Organize button on the dialog. Date and time ranges can be entered and are saved to the Settings.MDB so that they may be used again in future analyses.

Attachment A**Day of Week**

If a Day of Week field is available in the data, incidents included in the analysis may be limited to specific days of the week.

Options

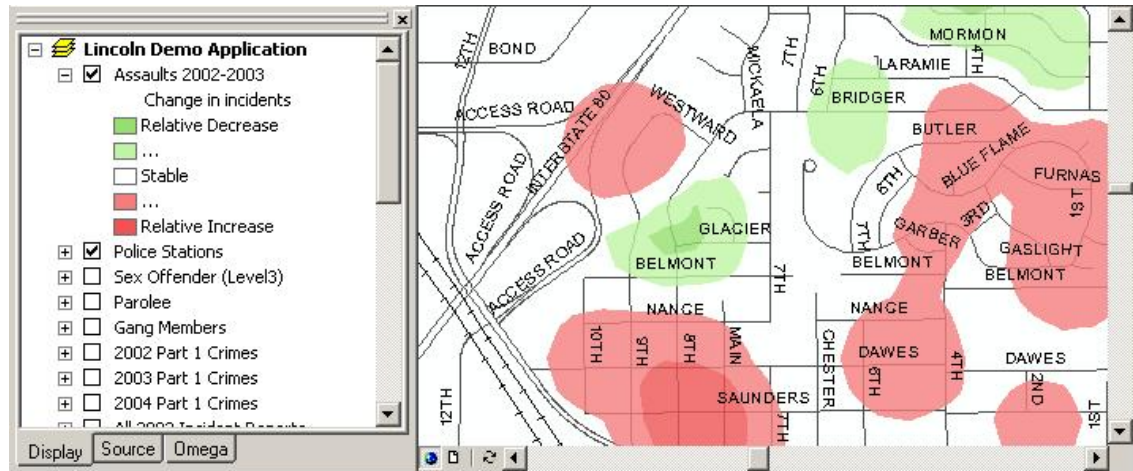
The fields on which date and time ranges are based may be selected using the Options button. To change the default date and time fields permanently, use the [OmegaGIS Metadata Editor](#) available within the OmegaGIS Data Manager extension in ArcCatalog.

About Spatial Trend Analysis**Availability by Extension**

CrimeView	FireView	School Planner
Spatial Trend Analysis	Spatial Trend Analysis	Spatial Trend Analysis

Spatial Trend Analysis is available in all of the products created by Omega, and can be used to look at changes in data that occur over time. In CrimeView, Spatial Trend Analysis can be used to identify whether the number of incidents in an area has increased or decreased. In FireView, the routine might be used to visually examine changes in the number of false alarms and false calls. Alternatively, in School Planner the analysis might provide a means to view whether student populations have increased or decreased over the years.

Although similar to [Exception Reporting](#) (Enrollment Comparison in School Planner) in that the result of the analysis is a comparison of historical data, Spatial Trend Analysis provides a few important differences. Spatial Trend Analysis is not limited to comparing a single layer of events. Multiple historical layers may be selected as the basis for evaluation, as well as specifying date and time ranges for each individual layer.

Attachment A

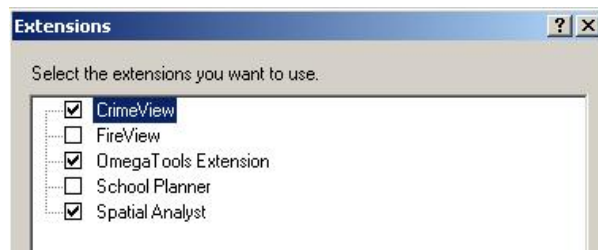
The quantitative results of Spatial Trend Analysis differ from Exception Reporting (Enrollment Comparison in School Planner) in that they are raster based as opposed to vector based. Changes in the data are compared cell by cell, and then interpolated to create contoured areas of change. Comparing events in this manner targets change, and does not stretch the results to the selected boundaries, as is the case when using the vector approach with Exception Reporting (Enrollment Comparison). Unlike the percentage results of Exception Reporting (Enrollment Comparison), Spatial Trend Analysis displays the output as classes of relative change based on the cell by cell calculations. The results create smooth relative changes calculated by the following expression:

$$[\text{Target Layer Raster}] - \text{Average} [\text{Historic Layer}_1 \dots \text{Historic Layer}_n] / n$$

Spatial Trend Setup

Extension Requirements

Spatial Trend Analysis is based on cell by cell calculations using raster layers. In order to perform these calculations, ESRI's Spatial Analyst Extension must be installed on the machine running the analysis, and the extension must be enabled. To check whether the extension is installed, click on the 'Tools' menu in ArcMap, and select 'Extensions' from the drop-down list. Spatial Analyst is shown in the list of extensions if it is available, and may be enabled by clicking on the checkbox.





In addition to Spatial Trend analysis, a few OmegaGIS routines require extensions supplied by ESRI. These extensions must be installed manually, however once on the machine, they can be enabled automatically by toggling a Global Setting in [OmegaGIS Setup](#).

Analysis Requirements

Target Layer

The target layer in the analysis, represents the layer that is compared to historical events in order to determine changes that have occurred over time. To appear in the list, the target layer must have a geometry type of point. Multipoint layers are not supported. The data source of the layer must be valid. If the data source is invalid, a red exclamation mark appears at the left hand side of the layer name in the ArcMap table of contents.

  2003 Part 1 Crimes

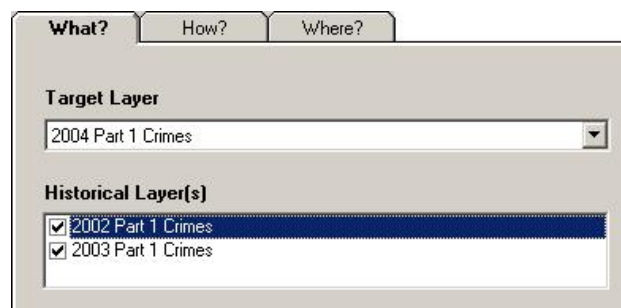
Selection layers are not included in the layer list. They are created as a result of running OmegaGIS routines. Selection layers share the same data as the layer on which they were based during the query. Consequently, including these layers in the layer list, essentially results in displaying duplicate data.

Often a project can become confusing with a growing number of layers in the table of contents. To avoid showing all of the layers in the OmegaGIS dialog layer lists, two options can be set using [OmegaGIS Setup](#). The first option deals with the use of registered layers. As layers are created, they can be registered as different types using the [OmegaGIS Metadata Editor](#) in ArcCatalog. Once registered, the setting 'Only use registered layers to create new queries' within the Queries settings in [OmegaGIS Setup](#) can be toggled to display only those layers registered as a specific type.

To limit the layer list further, those layers created by OmegaGIS routines may be excluded from the list explicitly using the 'Exclude layers...' checkbox on the Advanced tab of the Queries Settings. Setting this option ensures that layers created by any of the OmegaGIS routines are not listed in any of the layer lists for Spatial Trend Analysis.

Additional Query Layers

Additional Query Layers are point layers used as the historical comparison to the target layer. The list is populated based on the target layer selected. Additional query layers are only available to those target layers that share the same Query Groups and field list. However, they may include additional fields not found in the target layer. If no additional query layers exist for the selected target layer, Spatial Trend Analysis cannot continue.



The screenshot shows a dialog box with three tabs: 'What?' (selected), 'How?', and 'Where?'. Under the 'What?' tab, there are two sections: 'Target Layer' and 'Historical Layer(s)'. The 'Target Layer' section has a dropdown menu with '2004 Part 1 Crimes' selected. The 'Historical Layer(s)' section has a list box containing two items: '2002 Part 1 Crimes' and '2003 Part 1 Crimes', both with checked checkboxes.

Spatial Trend Dialog

Spatial Trend Analysis is composed of three types of questions that must be answered in order to produce results; which features should be selected (What?), what are the parameters to be used during the raster calculations (How?) and finally where is the geographic area of interest for the analysis (Where?). These questions are divided up as the What?, How? and Where? tabs on the Spatial Trend Analysis dialog.

[What Menu](#)

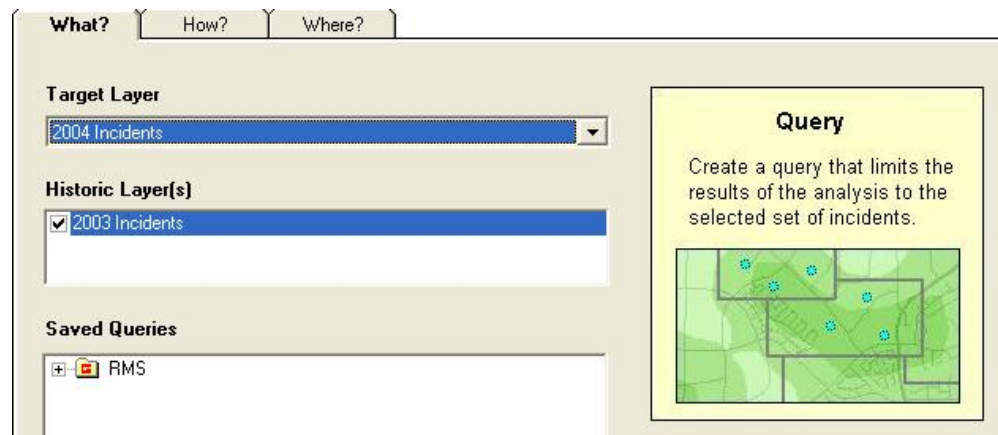
[How Menu](#)

[Where Menu](#)

[When Menu](#)

What?

The What? tab identifies which features to select for the subsequent Spatial Trend Analysis. Features are selected from a target layer and then compared to features selected from one or more [additional query layers](#). The features selected in each of these layers may be narrowed down further by using one or more queries from the [Saved Queries](#) Tree or Columns.



As there is no date/time query involved in Spatial Trend Analysis, it is important when comparing layers to ensure that the date range for each layer does not overlap.

How?

The How? tab contains a number of options that identify specific parameters required to set up both the input and output of the analysis.

Attachment A**New Layer Name**

The result of Spatial Trend Analysis is a new raster layer. The New Layer Name identifies the name that is displayed in the table of contents in ArcMap. A layer name must be entered in order to perform the analysis.

Map Color Scheme

The Map Color Scheme displays the results of the raster analysis as an array of predefined colors on the map. The default color scheme is Green to Red, where shades of green reflect decreases in the data and variations in red indicate a relative increase. Altogether four color schemes are available, however additional schemes may be created by modifying the [OmegaGIS.Style](#) file.

Population Field

The population field is essentially a weighting field that identifies the influence of data on the final analysis. For instance in CrimeView, violent crimes might be given greater weight than petty theft during an analysis to determine where to allocate additional personnel and resources.

Fields listed in the population field dropdown list are those that have a numeric field type. However, length and area fields are excluded.

The screenshot shows the 'What?' tab of the CrimeView 2002 application. It features three main sections: 'Target Layer' with a dropdown menu set to '2004 Incidents'; 'Historic Layer(s)' with a list containing '2003 Incidents' and a checked checkbox; and 'Saved Queries' with a list containing 'RMS'. To the right, a yellow 'Query' box contains the text: 'Create a query that limits the results of the analysis to the selected set of incidents.' Below this text is a small map showing a green area with blue star markers.

-

New Layer Extent

The New Layer Extent defines the outer boundaries of the resulting raster layer. The list includes 'Same as the Data Frame' and 'Same as the Current Extent'. The difference between these two choices is that the first uses the extent of the layer spanning the most area, while the second selection defines the envelope of the new raster as the current viewable area on the map. In addition to these two options, each of the layers within the table of contents is available as a basis for the extent of the new raster layer.

If the Subset by Boundary checkbox is checked, the New Layer Extent is no longer available. Instead, the new raster layer's extent will be based on the envelope surrounding the boundaries selected.

Cell Size

Attachment A

The new raster layer output by Spatial Trend Analysis is based on cell statistics. With this approach, the change in the data is calculated on a cell by cell basis. The default cell size for English units is 250 feet, while 75 meters is used for Metric units. The cell size must remain between 10 to 3280 feet when using English units or between 3 and 1000 meters when using Metric, if changing the cell size during a routine.

It is important to understand the implications of changing the cell size on the results of the analysis. Although decreasing the cell size may improve the resolution of the final result, it may also significantly impact performance. Conversely, increasing the cell size may enhance performance, but omit detail from the final analysis.

Search Distance

The search distance limits the data used to calculate the value of each cell by providing a maximum distance that will be searched for points around the center of the cell. The search distance should be set at 1.5 times the cell size. The default range of values falls between 15-13200 feet for English units or 5-4000 meters for Metric units. If the search distance entered is not within a valid range, it is recalculated during the routine to use the default values.

Reset

The Reset button can be used to set the cell size and search distance back to their default values.

-

Options

Two options are available for altering the placement of the new layer in the table of contents and the transparency of the new layer on the map.

Show Below Point and Line Layers

Selecting this checkbox places the new raster layer below point and line layers in the active data frame. By default the new layer is placed at the top of the table of contents, which may obscure features in the layers below.

-

Transparency

Transparency can be set to prevent the new layer from obscuring features in the layers below. Default values fall between 0 and 100, where 100 results in an invisible layer, and 0 is opaque. The default value is set at 20, allowing features below the new layer to remain visible. The transparency of the new layer may also be altered by using the Display tab in the Layer Properties dialog.

Where?

-

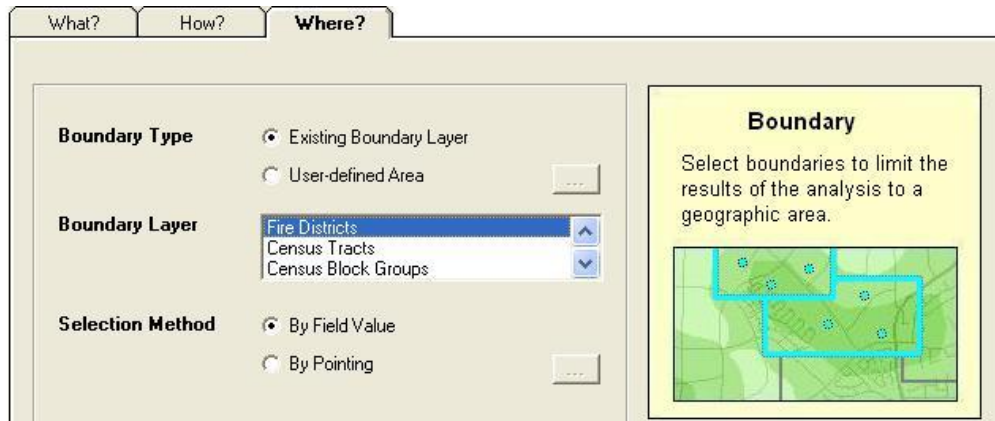
The Where? tab limits the raster analysis to a specific geographic region defined by either predefined or user-defined boundaries.

User-Defined Boundary

The user-defined boundary option is useful when no boundary layers exist on which to base the analysis. The ellipses button located next to the [User-Defined Boundary](#) option provides access to the map in order to delineate a polygon to use as the area of interest. For the routine to run, only one boundary can be selected, and its shape must be defined as a valid polygon.

Attachment A**Existing Boundary Layer**

When the existing boundary layer option is selected, the drop-down list is populated with valid polygon layers found in the table of contents. Boundaries from any of these layers may be selected either 'By Field Value' or 'By Pointing'. Multiple boundaries can be selected using both of these options.



When selecting boundaries 'By Field Value' the 'Select All' checkbox can be toggled to select each of the unique values in the list. The complete list button is used to increase the listing of unique values by sampling all of the polygons in the layer instead of the maximum number set in [OmegaGIS Setup](#).

When?

Not available in School Planner products.

The When? tab provides the functionality to add date, time, and day of week range query values to the target and historical layers, in order to restrict the incidents that are being used in the raster analysis calculation.

Attachment A

The screenshot shows the 'When?' tab of the CrimeView application. It is divided into two main sections: 'Target Layer' and 'Historical Layer(s)'. Each section has a list of layers on the left and a summary of date/time query information on the right. The 'Target Layer' section shows '2002 Part 1 Crimes' selected, with no date, time, or day of week queries set. The 'Historical Layer(s)' section shows '2003 Part 1 Crimes' and '2004 Part 1 Crimes' listed, with '2003 Part 1 Crimes' selected, and no date, time, or day of week queries set. Both sections have an 'Add Date/Time Query' button.

Section	Layer	Date Range	Time Range	Days of Week
Target Layer	2002 Part 1 Crimes	No Date Range Selected	No Time Range Selected	No Day of Week (DOW) Values Selected
Historical Layer(s)	2003 Part 1 Crimes	No Date Range Specified	No Time Range Specified	No Day of Week (DOW) Values Specified

The When? tab is arranged into two main sections, Target Layer and Historical Layers, based on the types of layers being used for the analysis. The only layers that will be available on the When? tab will be the ones that were selected to be used in the analysis on the What? tab. If a layer is not displaying, ensure that it has been selected for analysis on the What? tab, as it is not possible to change layers using the When? tab, but instead provides functionality only to add date and time queries to layers that have already been selected for analysis.

Within each section, a summary of the Date/Time Query information including the Date Range, Time Range, and Day of Week values set for that layer, is available. Since only one target layer is available for a Spatial Trend Query, the Target Layer section only displays the selected target layer query. Since multiple historical layers can be used when performing a spatial trend analysis, the selected layers from the When? tab are displayed in the list in the historical layers section. When a layer is selected in the list, the summary to the right will display any date and time information related to that layer.

In order to add a date/time query to a layer, select the layer (if it is a historical layer) and then press the appropriate Add Date/Time Query button. Note that if a date/time query is already present, then the button will say Edit Date/Time query instead. Pressing the button will bring up the following date/time query editor window:

Attachment A

The date/time query editor window is organized into the following areas, it is not necessary to set parameters for all areas of the date/time query.:

1. [Date](#)
2. [Time](#)
3. [Day of Week \(DOW\)](#)
4. [Predefined Date/Time Ranges](#)
5. [Previous Ranges](#)
6. [Other Controls](#)

1. Date:

Attachment A

FROM Date							TO Date						
◀ April ▶ ◀ 2006 ▶							◀ April ▶ ◀ 2006 ▶						
S	M	T	W	T	F	S	S	M	T	W	T	F	S
						1							1
2	3	4	5	6	7	8	2	3	4	5	6	7	8
9	10	11	12	13	14	15	9	10	11	12	13	14	15
16	17	18	19	20	21	22	16	17	18	19	20	21	22
23	24	25	26	27	28	29	23	24	25	26	27	28	29
30							30						

Use this section to apply a date range to the query, including month, day and year. Use the arrows next to the month and year indicators to scroll through the months and years, and select a calendar day by clicking on the day. The control will only allow dates which are present within the layers date range to be selected. Note however, that the viewer will default to the current date and so if the layer is historical it will be necessary to scroll back to the date range of the historical layer.

2. Time:

FROM Time	00:00	TO Time	00:00
------------------	-------	----------------	-------

Use the arrows to scroll through the time and to set the FROM and TO times. Times are displayed in a 24 hour format. If no range is set (00:00 to 00:00) then a time range will not be used in the query.

3. Day of Week (DOW):

Day of Week	
<input type="checkbox"/>	Sunday
<input type="checkbox"/>	Monday
<input type="checkbox"/>	Tuesday
<input type="checkbox"/>	Wednesday
<input type="checkbox"/>	Thursday
<input type="checkbox"/>	Friday
<input type="checkbox"/>	Saturday

Simply check off the days of week which are necessary for the query. If no days are checked then no Day of Week values will be used in the query.

4. Predefined Date/Time Ranges:

Attachment A

The image shows a user interface with two sections. The first section is titled "Predefined Date Range" and contains a dropdown menu with "ALL DATES" selected and an "Organize..." button. The second section is titled "Predefined Time Range" and contains a dropdown menu with "ALL TIMES" selected and an "Organize..." button.

It is possible to store predefined date and time ranges in order to retrieve them if they are used frequently with the same settings. This is done using the Predefined Date Range and Predefined Time Range controls. The drop-down lists are pre-populated with the following predefined ranges including:

All Dates: Select all of the dates available in the layer.

Other (Default): Use to manually set the date range.

Today: Select just the current day.

Week to Date: Select all of the days in the current week to the current day.

Month to Date: Select all of the days in the current month to the current day.

Year to Date: Select all of the days in the current year to the current day.

The Predefined Time Ranges offer the following settings:

All Times: Equivalent to not setting a range.

Other (Default): Use to manually set a time range.

Day: Daytime hours between (06:00 to 17:59).

Night: Nighttime hours between (18:00 to 05:59).

The purpose of using predefined date and time ranges is simply to save time in selecting commonly or frequently used date and time queries.

It is also possible to build custom Predefined Date and Time Ranges. For additional help regarding this, see the section in this document titled: [Working with Custom Date and Time Ranges](#).

5. Previous Ranges:

The image shows a user interface element with the label "Previous" followed by two dropdown menus. The first dropdown menu is empty, and the second dropdown menu has "Days" selected.

Attachment A

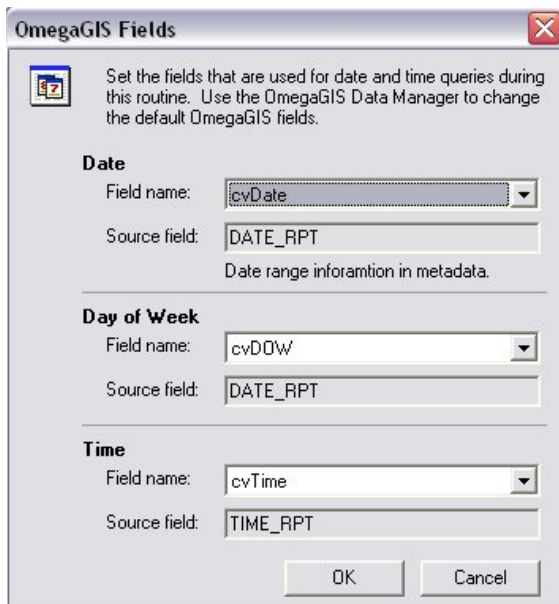
The Previous section allows a duration of a time period, defined in either hours, days, weeks, months, or years to be set using the current date as the end date. This is a fast way to enter the information if a date or time range up the current date or time is needed. Select the number of date time units from the first drop down list and then select the date or time units from the second one.

6. Other Controls:

The Other Controls on the page include the Clear All and Options... buttons, as pictured above.

Clear All: Resets the date/time query controls and clear all of the stored query information for the layer.

Options...: Opens the following dialog which allows the selection of which fields to use in the date/time query calculation.



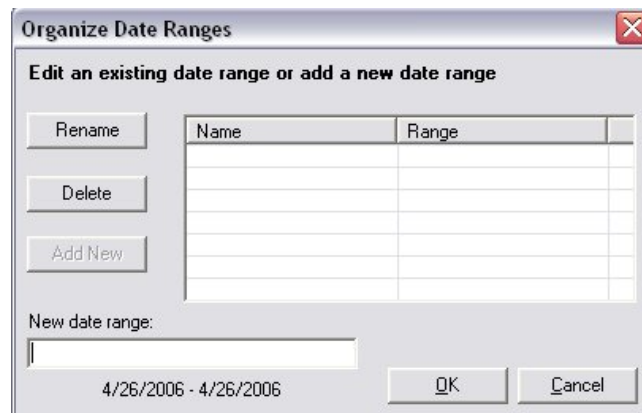
To change the field to use, select the field from the drop-down menu for the appropriate parameter, either Date, Time, or Day of Week. Note that only fields which have been registered in the layers metadata as additional date/time fields can be selected from this list. In order to access OmegaGIS metadata, use the OmegaGIS Metadata Editor, available through the OmegaGIS Data Manager Toolbar in ArcCatalog. The default field can also be changed in the Metadata Editor.

Working with Custom Predefined Date and Time Ranges

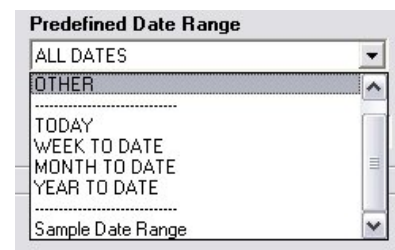
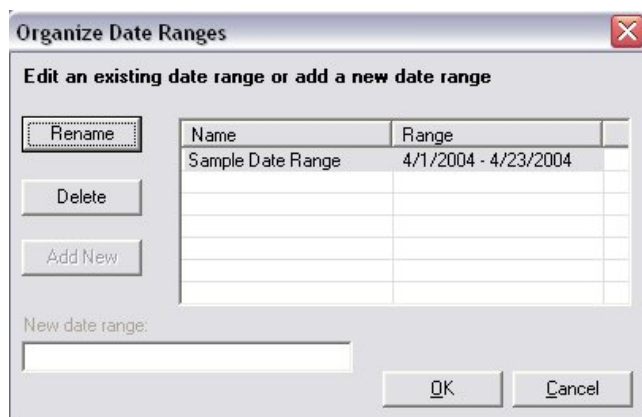
Custom predefined Date and Time ranges can be created in OmegaGIS by using the Organize... functionality beside the Predefined

Attachment A

Date Range list. This brings up a window that allows the modification of or creation of predefined date or time ranges.

**Setting a new Date or Time range:**

In order to set a date or time range, first set the range as normal on the Date and Time Query controls before opening the appropriate Organize Range button. For additional help on using the controls found on the When? tab, see the [When?](#) section in this help document. When a custom range is set on the Date and time dialog, the default option on the Predefined Date Range, or Predefined Time Range window will change to "OTHER". When OTHER is selected, then the option to edit or add a date range will be available when the Options... button is pressed. Once the date or time range to store has been set, select the appropriate Organize... button to open the Organize Date or Time Ranges dialog. If there are no previously stored ranges, then the list of available ranges will be empty (as in the image above) and the range selected will be displayed at the bottom of the form. Give the stored range a name by entering it in the "New date range" text box, and press the "Add New" button. The range is now stored and will be selectable from the respective Predefined Date Range or Predefined Time Range drop down lists on the main Date and Time Query window.



The Organize [Date/Time] Ranges menu also provides functionality to either rename or delete previously created Date or Time ranges. To rename or delete the date or time range, use the Organize... button to open the appropriate Organize Range dialog and then select the Range to rename or delete from the list. Use either the "Rename" or "Delete" button to perform the desired action, then press OK to exit the Organize Date Ranges window.

Spatial Trend Results

Map Layer

The result of a Spatial Trend Analysis is a new map layer that identifies whether changes in the data have occurred over time. The new layer is based on cell statistics performed on the raster data generated by the analysis.



In this process, the Target Layer is first converted to a raster layer using the parameters entered into the dialog. Kernel Density is used as the method to create the raster layer. In this method, a smoothly curved surface is fitted over each point. The kernel value is highest directly over the point, and diminishes outward to zero when the search radius distance is reached. The density of each raster cell is calculated by adding the values of all kernel surfaces within the cell, provided they overlay the cell center. If the Population field is used then the population value found for each point encountered is used to weight the individual point. For example, if a value of '4' is found, then the point is counted as four points before the raster density is calculated.

After the Target Layer is calculated, Kernel Density is used to create the raster layers for each of the Historic Layers used in the analysis. Once these raster layers are created, the raster results are averaged together to create the 'mean' historic raster layer. At this point, cell statistics are performed using the following equation:

$$[\text{Output Raster}] = [\text{Target Raster}] - [\text{History Raster}]$$

To display the new raster layer, bilinear interpolation is used as the resampling method. This method samples four of the neighboring raster cells to produce an average for each raster cell in the layer. Averaging cells in this manner produces a smoother surface as a result.

Map Legend

Attachment A

The map legend illustrates the categories that are used to display the Spatial Trend raster results. The legend is always divided into five classifications ranging from 'Relative Decrease' to 'Relative Increase'. These classifications are generated using Jenk's Natural Breaks method of classification.

The Natural Breaks method subsets similar data values into classes by determining the partitions for these classes based on a statistical formula (Jenk's optimization). The partitions or breakpoints are calculated by finding the sum of absolute deviations about the class median, or alternatively, the sum of squared deviations about the class mean.

Although Omega uses the Natural Breaks method for classification, careful study of the data may indicate that other classification methods are more appropriate. The method of classification can be changed after the analysis is run by accessing the Symbology tab from the Properties page of the new raster layer.

The following information is taken from the ESRI Online Help, and provides a brief summary of the classification methods available:

"There are several different classification methods you can choose to organize your data when doing thematic mapping. These include equal interval, natural breaks, quantile, equal area, and standard deviation.

*In the **Equal Interval** classification method, each class has an equal range of values; that is, the difference between the high and low value is equal for each class. You should use this method if your data is evenly distributed and you want to emphasize the difference in values between the features.*

*With the **Natural Breaks** classification method, data values that cluster are placed into a single class. Class breaks occur where there is a gap between clusters. You should use this method if your data is unevenly distributed; that is, many features have the same or similar values and there are gaps between groups of values.*

*With the **Quantile** classification method, each class has roughly the same number of features. If your data is evenly distributed and you want to emphasize the difference in relative position between features, you should use the quantile classification method. If, for example, the point values are divided into five classes, points in the highest class would fall into the top fifth of all points.*

*With the **Equal Area** classification method, classes are formed so that the total area in each class is approximately the same (available only when working with areas).*

*With the **Geometrical Interval** classification method, class breaks are based on class intervals that have a geometrical series. The geometric coefficient in this classifier can change once (to its inverse) to optimize the class ranges. The algorithm creates these geometrical intervals by minimizing the square sum of element per class. This ensures that each class range has approximately the same number of values with each class and that the change between intervals is fairly consistent. This algorithm was specifically designed to accommodate continuous data. It produces a result that is visually appealing and cartographically comprehensive.*

*With the **Standard Deviation** classification method, class breaks are placed above and below the mean value at intervals of 1, 0.5, or 0.25 standard deviations until all the data values are included in a class."*

Map Data Source

Attachment A

The data source for the new layer is stored in the \hotspot folder within the project directory structure. When a new raster layer is created, the raster data source name is created with a consecutive numbering system; raster1, raster2 etc. This name is created automatically during the processing.

◇ Project Clear All

Availability by Extension

CrimeView	FireView	School Planner
Clear All	Clear All	Clear All

Project Clear All is used to reset the project to its original state based on options set in [OmegaGIS Setup](#). Clearing the project includes removing layers generated by OmegaGIS routines, removing selection sets and graphics, and resetting the map view.

Access to Project Clear All is available from both the CrimeView dropdown menu, as well as the CrimeView toolbar. The following events take place when using the Project Clear All.

[Selection Layers Removed](#)

[Turn Off Selection Layers](#)

[Set Visibility of Registered Query Layers](#)

[Set Selectability of the Layers](#)

[Clear Omega Feature Definitions](#)

[Remove Additional Query Layers](#)

[Clear Selection Sets](#)

[Remove OmegaGIS Graphics](#)

[Zoom to the Project Bookmark](#)

[Save Map as Thumbnail](#)

[Remove OmegaGIS Layers from Map](#)

Attachment A**Selection Layers Removed**

Selection layers are the result of running the [Query](#) routines provided with OmegaGIS . A selection layer is not distinct, but is linked to the source data on which it is based. For instance, the data source of a new layer showing only those crimes classified as assaults, actually leads back to the Part 1 Crimes layer from which the assault crimes were drawn.

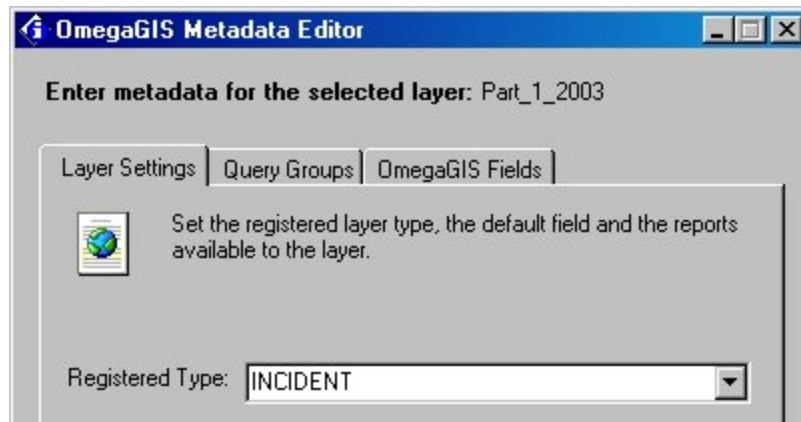
Selection layers are identified in the Table of Contents with the text (Selection) placed after the layer name. A selection layer may also be identified by right-clicking on the Properties dialog and selecting the Definition Query tab. The text “*Layer based on a selection set...” identifies the layer as a selection. Depending on the setting in [OmegaGIS Setup](#) all Selection Layers are removed from the Table of Contents when the Project Clear All is run.

**Turn Off Selection Layers**

Instead of removing Selection Layers, they may be turned off by setting the appropriate option in [OmegaGIS Setup](#).

Set Visibility of Registered Query Layers

Registered Query Layers are those layers that have been assigned a registered type using the [OmegaGIS Metadata Editor](#). Although any name can be used as a registered type, currently OmegaGIS only recognizes 'Incident', 'Person', 'Student' and 'Other'. Consequently, if the 'Use registered type...' setting is selected in [OmegaGIS Setup](#), only those layers matching a registered type of 'Incident', 'Person', 'Student' or 'Other' will show up in the layer list of an OmegaGIS routine. Layers registered with different names are excluded.

Attachment A

During the 'Project Clear All' event, the visibility of the Registered Query Layers is controlled based on two settings in OmegaGIS Setup. The 'Turn off visibility of registered query layers' setting controls the visibility of the 'Incident', 'Person' and 'Student' layers, while the 'Turn off visibility of the layers registered as 'Other' option controls the visibility of layers registered as 'Other'.

Set Selectability of the Layers

The selectability of a layer refers to whether features in the layer can be selected on the map. Depending on the setting in [OmegaGIS Setup](#), layers can be set to retain their selectability or automatically set to unselectable .

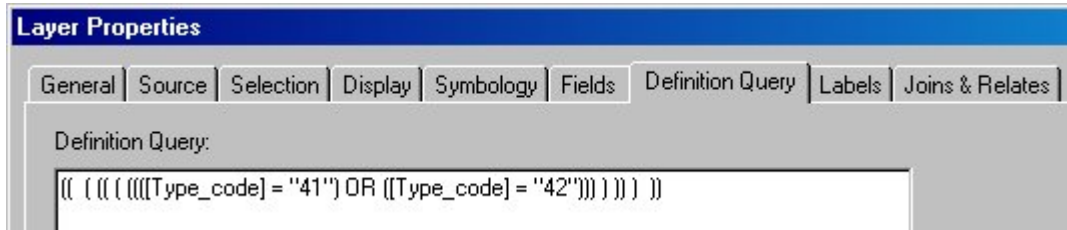


Clear Omega Feature Definitions

A feature definition is used in ArcMap to display features based on an attribute query. Only those features that obey the query are shown on the map. In OmegaGIS , this method is used as well when an OmegaGIS [Query](#) routine is run. If the setting 'Show only saved query values and highlight selection' is selected in [OmegaGIS Setup](#), only those features selected by the query in the routine are displayed on the map.

Attachment A

An Omega Feature Definition is simply the query used to identify the output features of an OmegaGIS routine. An Omega Feature Definition can be recognized by right-clicking on the layer name in the Table of Contents, clicking Properties, and selecting 'Definition Query'. An Omega Definition Query is delimited by a unique set of brackets '((((((((((Omega Query Here))))))))))'.



During a Project Clear All, these feature definitions can be removed by setting an option in [OmegaGIS Setup](#).

Remove Additional Query Layers

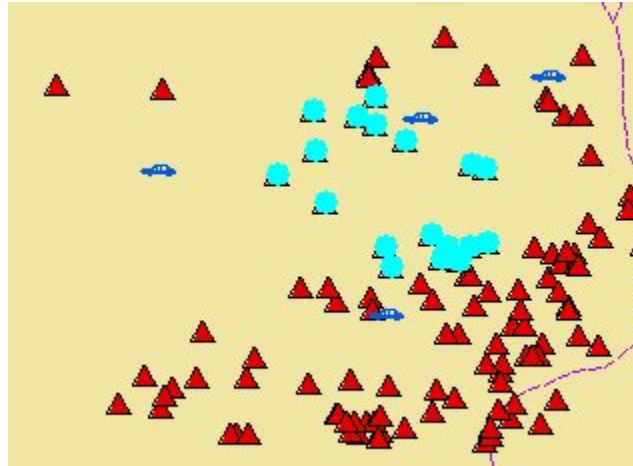
[Composite layers](#) are created when more than one layer is combined during an OmegaGIS routine. The layer can be recognized in the Table of Contents by the term '(Composite)' that is added to the layer name.



Composite layers may be removed from the project during a Project Clear All by setting the appropriate option in [OmegaGIS Setup](#).

Clear Selection Sets

While querying the data, selection sets may be created to identify the results of the query. Features that appear highlighted on the map, are those that have been added to a selection set. During a Project Clear All, every layer is cleared of any selection sets placed on it.



Remove OmegaGIS Graphics

In the case of OmegaGIS routines that create labels and buffers, these graphics are added to two distinct annotation layers called 'OmegaGIS Buffer' and 'Omega Label >'. During a Project Clear All, graphics from both of these layers are removed if the setting is selected in [OmegaGIS Setup](#).

Zoom to the Project Bookmark

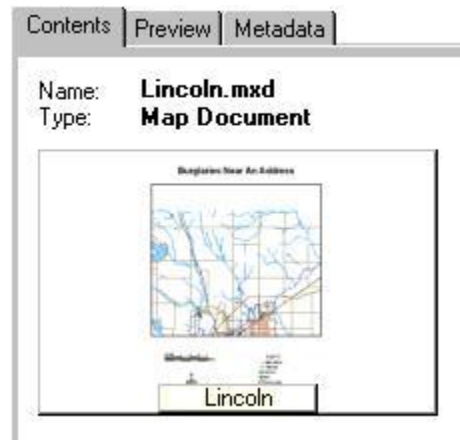
The Project Bookmark can be set to either Full Extent or Home. The Project Bookmark identifies the extent that the map will zoom to during the Project Clear All event. Zooming only takes place if the option is set in [OmegaGIS Setup](#).

Save Map as Thumbnail

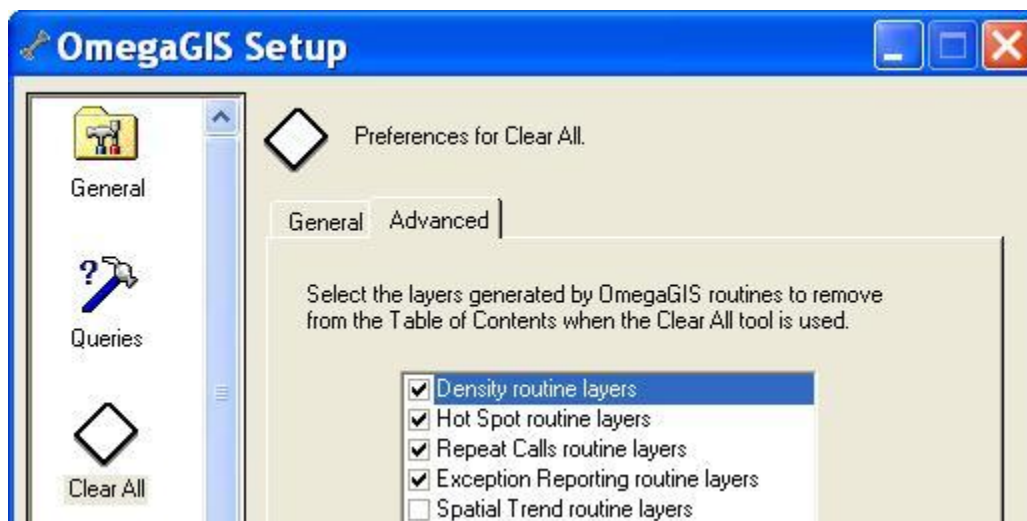
A map thumbnail can be used when viewing the project data using ArcCatalog . It provides a quick visual overview of the data contained within the project. Project Clear All creates the thumbnail, provided the option is set in [OmegaGIS Setup](#). It is recommended that this option not be set as it

Attachment A

impedes performance when closing ArcMap .

**Remove OmegaGIS Layers from Map**

Within OmegaGIS Setup, the Advanced Tab of the ClearAll settings is available in order to select specific OmegaGIS layers that should be removed from the map's Table of Contents when the ClearAll tool is used. Each routine and tool that generates layers can be specifically selected to remove only those layers from the map.

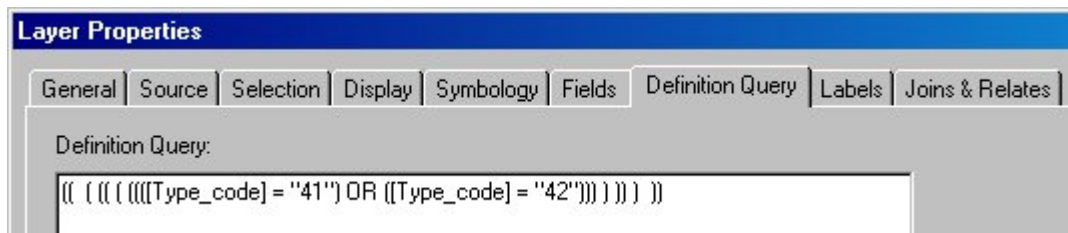


Clear OmegaGIS Definitions

Availability by Extension

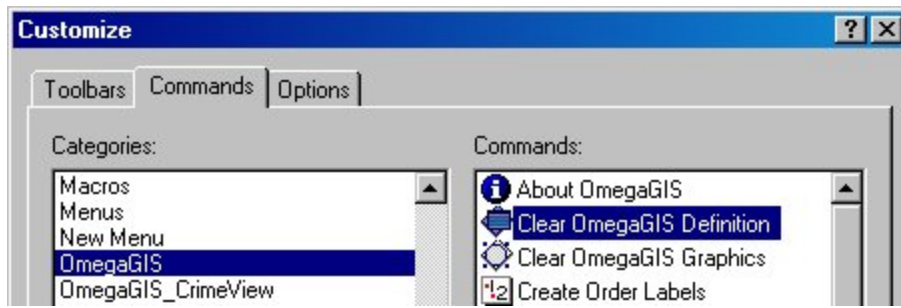
CrimeView	FireView	School Planner
Clear Definitions	Clear Definitions	Clear Definitions

A feature definition is essentially a filter that enables the display of features meeting specific criteria while hiding those that do not. An OmegaGIS Definition is generated when one of the OmegaGIS [Query](#) routines is run. This definition query can be recognized by the special characters that delimit the query.



By right-clicking on the layer name in the table of contents, and selecting 'Properties', the 'Definition Query' statement that is used to filter features can be viewed. An OmegaGIS Definition query is delimited by the following series of brackets (((((((Omega Query))))))). By using a unique series of characters, the Clear OmegaGIS Definitions utility can remove those filters applied by OmegaGIS routines, while leaving queries created directly in ArcMap intact.

This feature is not available on the OmegaGIS toolbar but can be accessed using the 'Customize' menu item from the 'Tools' menu. The utility is found in the Commands tab, within the OmegaGIS category.



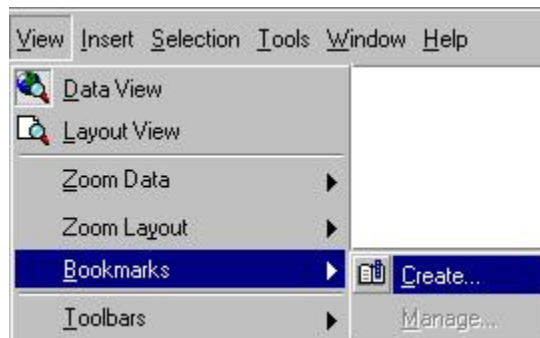
Go To Home

Availability by Extension

CrimeView	FireView	School Planner
Go To Home	Go To Home	Go To Home

The Go To Home button is available on an Omega GIS toolbar, such as CrimeView. The utility is based on the concept of Bookmarks in ArcMap. A bookmark is a spatial place holder that is defined by a specific map extent. Bookmarks can be placed anywhere on a map, and once they are set up, they provide a quick method for zooming quickly to locations in the project.

The Go To Home utility uses the map extent employed by the HOME bookmark. Each time the Go To Home button is used, the project's active view is reset to the user defined map extent of the HOME bookmark. To create the HOME bookmark, in ArcMap, select the 'View' menu, 'Bookmarks', and 'Create'.

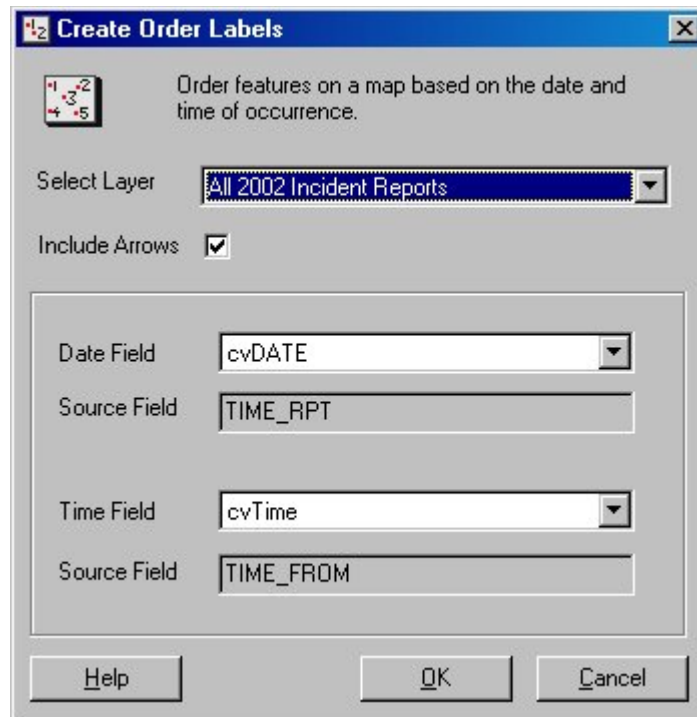


 **Create Order Labels****Availability by Extension**

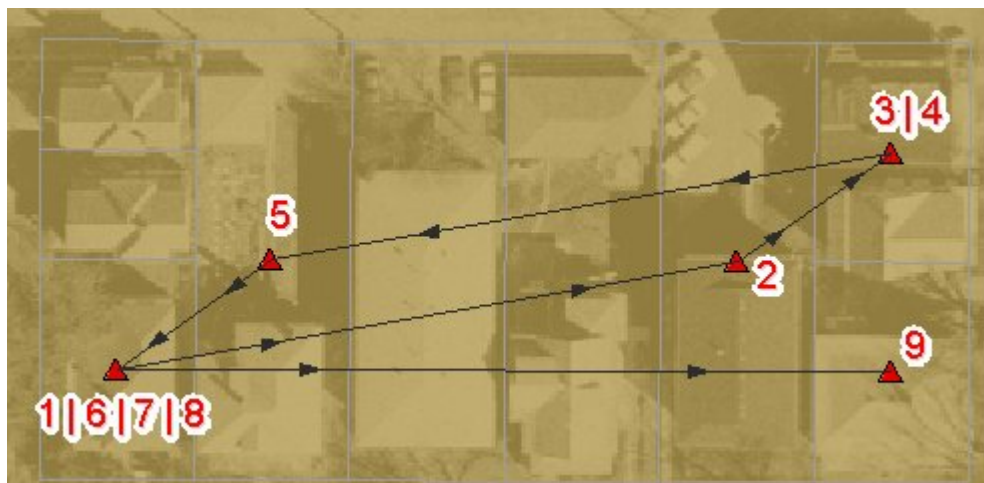
CrimeView	FireView	School Planner
Create Order Labels	Create Order Labels	Not Available

Create Order Labels is available from the OmegaGIS dropdown menu. The utility provides a quick method for viewing the chronological order of a series of events. A layer must be selected from the list provided. The layers that populate the list are those containing OmegaGIS date fields on which a chronological order can be based. If multiple date fields exist, the fields of interest may be selected from the dropdown lists.

Attachment A



The resulting graphics that are created by the routine include a numbering of the events, as well as directional arrows. Arrows are only displayed if the option is selected on the dialog. The symbology of the text is based on that of the source layer. Use the layer properties 'label' tab to set the symbology for the base layer, and consequently for the labelling that is used by the Create Order Labels tool.

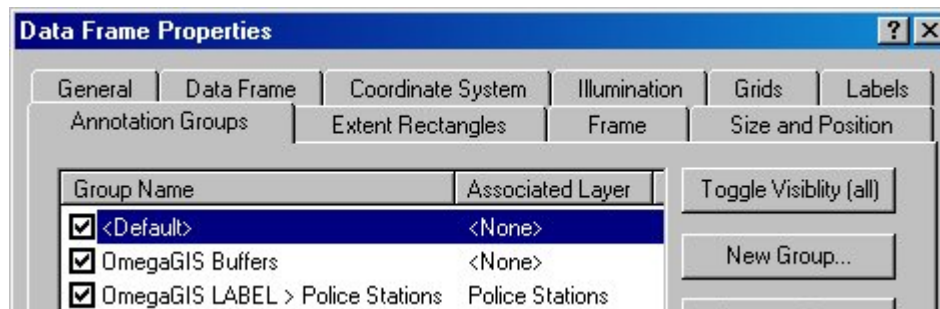


Remove OmegaGIS Graphics

Availability by Extension

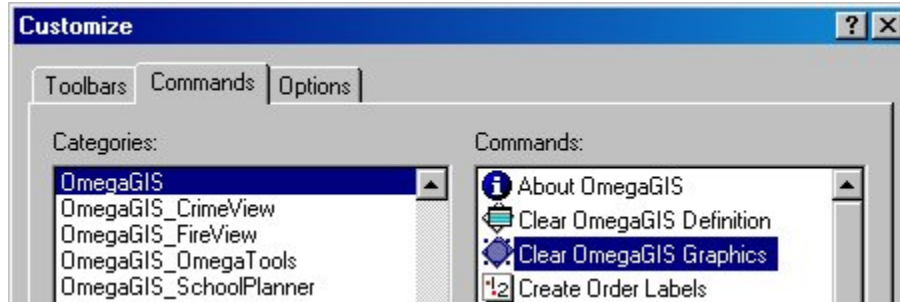
CrimeView	FireView	School Planner
Remove OmegaGIS Graphics	Remove OmegaGISGraphics	Remove OmegaGIS Graphics

Some OmegaGIS routines and tools include options for generating graphics when the results are displayed. When graphics are added to the output of an OmegaGIS routine, the resulting labels and/or buffers are placed in two new annotation layers called 'OmegaGIS Buffer' and 'Omega Label >'. The layers ensure that graphics created by OmegaGIS do not become confused with graphics created directly through the ArcMap interface.



The Remove OmegaGIS Graphics utility can be used to eliminate only those graphics created in running OmegaGIS routines and tools. Graphics created through the ArcMap interface remain intact.

This feature is not available on the OmegaGIS toolbar but can be accessed using the 'Customize' menu item from the 'Tools' menu. The utility is found in the Commands tab, within the OmegaGIS category.

Attachment A

Statistical Profiler

Availability by Extension

CrimeView	FireView	School Planner
Statistical Profiler	Statistical Profiler	Not Available

Overview

Statistical Profiler is a statistical tool for profiling crime series data. Running the statistical profiler results in the creation of rectangular polygons on a map, outlining the area where the next incident in a series is likely to occur. In addition to the new probability rectangles, a report is generated indicating the most likely occurrence of the next crime.

Before using this utility, a crime series should be identified that shows some logical link between the crimes in question. These crimes can either be selected from a layer, or created as a new selection layer by using one of the OmegaGIS [Query](#) routines.

The Statistics

For the purpose of this utility, it is assumed that the data is normally distributed. With this

Attachment A

assumption in place, the mean and standard deviation of the X and Y coordinates for the selected incidents are calculated. The three rectangles created in the analysis represent three standard deviations from the mean.

In general, sample data sets that are found to be normally distributed are based on standard deviations of 68%, 95% and 99.7%. In this case however, where we are dealing with probability distributions for a rectangular area, the standard deviation must be calculated for both an X and Y direction. Consequently, the standard deviations of 46%, 90% and 99% are used instead. These figures are calculated by multiplying the original standard deviations together to create $.68 \times .68 = .46\%$, $.95 \times .95 = .90\%$ and $.997 \times .997 = .99\%$.

**Selecting a Query Layer**

The first task in performing a statistical analysis on a layer is to select the layer of interest. Only point or multipoint feature layers are available in the drop-down list. In addition, if the 'Use Registered Types' setting is checked in [OmegaGIS Setup](#), only those layer types matching those selected in Setup are available. To edit or view a feature layer's registered type, the [OmegaGIS Metadata Editor](#) tool may be used from within ArcCatalog.

To run the analysis on a selection set within the feature layer, select the 'Selected records only' checkbox on the dialog. An example of a selection set of incidents might include a subset of burglaries with similar Modus Operandi (MO).

Selecting an Output Type

The results of the analysis can be output to the map as a layer or graphic. When creating a new layer, the advanced button can be used to set the placement of the new layer within the table of contents, and the transparency.

Attachment A

If 'Graphic' is selected, the results are placed in an annotation layer called 'OmegaGIS Buffers'. The new annotation layer may be viewed by right-clicking on the data frame, and selecting 'Properties'. Turning the annotation layer on and off, toggles the display of the new graphics. These graphics are also associated with the layer on which the analysis is based. Turning off this layer, turns off the graphics on the map.

**Date Time Profiler**

Provided that the attributes of the selected feature layer include OmegaGIS date and time fields, the Date-Time Profiler analysis may be run. The routine estimates the probable date and time range for the next crime in a series, based on the data selected.

The routine calculates the mean (average) number of days between occurrences and the standard deviation, assuming a normal distribution. The standard deviation represents the amount the mean will differ from the true population mean, given a 68% confidence interval.

The mean number of days is then added to the date of the last occurrence. The upper and lower limits of the next expected occurrence are based on one standard deviation from the mean date. The same process is used to estimate the time frame of the next occurrence.

-



Attachment A**Advanced**

If there are multiple OmegaGIS fields in the data, it is possible to select the field to use during the Date-Time Profiler analysis using the Advanced button. The Advanced dialog provides the opportunity to both select the field, and view the source field on which the OmegaGIS field is based.



Create Reports

Availability by Extension

CrimeView	FireView	School Planner
Create Reports	Create Reports	Create Reports

The Create Reports tool is the central location for creating formatted reports presented in a custom Crystal Reports Viewer. The Crystal Reports Viewer allows the user to view and navigate through the report, zoom in and out, change printer settings, print and export.

[Select Layer](#)

[Select Crystal Report](#)

[Generate Report](#)

Select Layer

When the Create Reports dialog is opened, each valid layer in the active data frame that has a registered Crystal Report is added to the list of layers on the dialog. The type of layers that are available in the list are identified by a unique icon placed before the layer name and include:

- ***Query Layers***

Crystal Reports can be registered to [Query Layers](#) (point feature classes) using the [OmegaGIS Metadata Editor](#). There is no limit as to the number of Crystal Reports that can be registered to a Query Layer. Selection layers and [Composite layers](#) created by [query routines](#), such as Incidents Within A Boundary, are also added to the list of layers on the dialog provided that their parent layer had a registered Crystal Report.

If the selected Query Layer has selected features the 'Selected records only' check box is enabled and is checked by default. When checked, only the selected records are exported and used to generate the Crystal Report, otherwise all of the records in the layer are used.



- ***Repeat Calls Layers***

The [Query Layer](#) that is used to generate the [Repeat Calls](#) layer must have one and only one Repeat Calls Report registered to it. The [OmegaGIS Metadata Editor](#) in ArcCatalog is used to register a Repeat Calls Report to a layer.



OmegaGIS Metadata Editor

When the Repeat Calls layer is created, the information on the Repeat Calls Report from the Query Layer is copied to the new layer. The registered Repeat Calls Report can be altered on an existing Repeat Calls layer by using the OmegaGIS Metadata Editor.

Attachment A

Unlike reports for Query Layers, all of the features in the Repeat Calls layer are used in the report. The "Selected records only" checkbox is always disabled on the dialog.

- ***Density Map Layers***

The Density Map Crystal Report provides a statistical summary of the count and density values in order to identify statistical outliers or potential problem areas.

The polygon layer that is used to generate a [Density Map layer](#) must have one and only one Density Map Crystal Report registered to it. The [OmegaGIS Metadata Editor](#) in ArcCatalog is used to register the Density Map Crystal Report to a layer.

Similar to the Repeat Calls layer, when the Density Map layer is created, information on the Density Map Crystal Report is copied to the new layer. The registered Density Map Crystal Report can be altered on an existing Density Map layer by using the OmegaGIS Metadata Editor.

Similar to Repeat Calls, all of the features in the Density Map layer are used in the report. The "Selected records only" checkbox is always disabled on the dialog.

When the dialog is opened, the layer that is currently selected in table of contents is selected in the list, provided that the layer has a registered report.

Select Crystal Report

When a layer is selected, the list of registered Crystal Reports is populated. The location(s) of the reports is set using [OmegaGIS Setup](#). There can be one or more locations for reports. The locations are searched in the order they are defined in OmegaGIS Setup until a Crystal Report whose name matches the registered report is found. Only registered reports names are shown in the list; to get the full path of a Crystal Report hover the mouse over the report and a tool tip appears showing the full path. Reports that are not found are preceded with the report icon with a red 'X'.



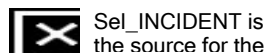
When a valid Crystal Report is selected the 'OK' button is enabled.

Generate Report

The Crystal Report Viewer is opened and displays data from the selected layer when the 'OK' button is clicked. The source of the data for the report is dependent upon the type of layer selected.

- **Query Layer**

Depending on the users specifications, either all of the layers records or only the selected records are exported to the 'Sel_INCIDENT' table in the Selection.MDB located in the [project workspace](#). All of the fields in the Query Layer, excluding the geometry, are exported to the Selection.MDB.



Sel_INCIDENT is
the source for the

The Selection.MDB is automatically created if it is not present in the project workspace. If the 'Sel_INCIDENT' table already exists in the Selection.MDB it is deleted and replaced.

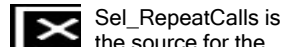
- **Repeat Calls Layer**

All of the records from the source Query Layer that were used to generate the Repeat Calls layer are exported to a point feature class named 'Sel_RepeatCalls' in the Selection.MDB located in the [project workspace](#). The 'Sel_RepeatCalls' is used as the source of the Crystal Report. When [additional query layers](#) are used to create the Repeat Calls layer, the records are exported from the RC_AddQueryLayer_* feature class located in the [RepeatCalls.MDB](#).

A spatial filter is used to determine the records from the source Query Layer that were used to

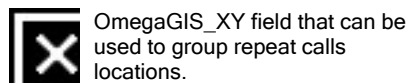
Attachment A

generate the Repeat Calls layer. This spatial filter contains the attribute query, if any, that was used along with the geometry from the repeat call locations. The point geometry of the repeat calls locations is buffered before being placed in the spatial filter; the buffer distance is controlled by a parameter that is set in the [project setup](#).



The Selection.MDB is automatically created if it is not present in the project workspace. If the 'Sel_RepeatCalls' feature class already exists in the Selection.MDB it is deleted and replaced.

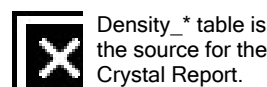
The 'Sel_RepeatCalls' table has a field in it called "OmegaGIS_XY". The values in this field can be grouped in Crystal Reports to determine the repeat call locations.



When the Repeat Calls Report is opened, the Repeat Calls layer is made visible and any selected features are cleared. Any other Repeat Calls layers in the table of contents are made invisible.

- ***Density Map Layer***

The source of the Density Map Crystal Report is the 'Density_*' feature class located in the [DensityMap.MDB](#) in the Density folder in the [project workspace](#). The source table of the report is dynamically updated to use the appropriate table in the DensityMap.MDB.



The 'Density_*' table contains all of the boundary layer fields plus two new fields that are created by the Density Map routine that can be used in the report.

Attachment A*OmegaGIS_Count*

This field contains the number of incidents that are found in the boundary.

OmegaGIS_Density

The density (count of incidents / area) is in this field. The area is calculated in square kilometers or in square miles, depending on the measurement system selected in the [OmegaGIS Setup](#) dialog.

The "Shape_Area" field is not used in the calculation of the OmegaGIS_Density field. The "Shape_Area" field is created and maintained by the Geodatabase and the values in this field are in the units of the spatial reference of the feature class which may not be in Kilometers or Miles.

Tip: If there are no records in the report, click the Refresh button in the Crystal Report Viewer.

Create Graphs

Availability by Extension

CrimeView	FireView	School Planner
Create Graphs	Create Graphs	Create Graphs

The Create Graphs button is used to create three dimensional graphs for [Query Layers](#).

Attachment A[Select Layer](#)[Select Graph](#)[Change Default Fields](#)[Generate Graph](#)**Select Layer**

When the Create Graphs dialog is opened, each layer in the active data frame is added to the list if it is a valid point layer. When a layer is selected, the Select Graphs list box is populated with the graphs that are available to the layer.



If the layer has selected features, the 'Selected records only' check box is enabled and is checked by default. If this box is checked when the routine is run, only the selected records are exported and used to generate the graph. Otherwise, the graph is generated using all of the records.

**Select Graph**

There are 6 standard three dimensional graph templates available with Omega GIS.

Attachment A**7-24 Graph**

The 7-24 Graph is a vertical bar chart counting selected points by what time and day of the week they occurred. This graph requires an OmegaGIS date field and time field.

Incident Type Graph

Incident Type Graph is a vertical bar chart counting selected incidents for each incident type. This graph requires a field identified as the Incident Type Graph Field in the layers metadata. This graph is always available, if there is no metadata information on the Incident Type Graph Field, then one is prompted when the 'OK' button is selected.

Day of Week Graph

The Day Of Week Graph is a vertical bar chart counting selected incidents by the day of the week they occurred. This graph requires an OmegaGIS day of week field.

Month of Year Graph

The Month of Year Graph is a vertical bar chart counting selected incidents by the month they occurred. This graph requires an OmegaGIS date field.

Time of Day Graph

The Time Of Day Graph is a vertical bar chart counting selected incidents by the hour of the day they occurred. This graph requires an OmegaGIS time field.

Response Time Graph

This graph is a vertical bar chart counting the selected incidents by the response time. This graph requires an OmegaGIS Response Time 2 field. The Response Time 2 field is generated using the Omega Import Wizard or the OmegaGIS Fields Manager. This field contains the same results as the Response Time field but includes 2 decimal places in the calculations.

Change Default Fields

OmegaGIS fields are used in the creation of the graphs. Default OmegaGIS fields set initially with the [OmegaGIS Metadata Editor](#). These fields can be altered by clicking on the Fields button to open a

Attachment A

dialog. The dialog allows one to change the default fields to other fields available in the selected layer.

The list of fields are populated based on information from the layer's metadata. This metadata information is set with the Omega Import Wizard or the OmegaGIS Field Manager. To alter the field to be used in the creation of the graph, change the appropriate list and click OK to close the dialog.



Change the default OmegaGIS field used in the creation of the graph.

The Incident Type field is any text or numeric field that is used in the graph to display the number of incidents per incident type. The default Incident Type field is set with the [OmegaGIS Metadata Editor](#). If the default Incident Type field has not been set, then the 'cvLegend' field is used when present in the layer.

Generate Graph

The selected graph(s) are opened displaying data from the selected layer when the 'OK' button is clicked. Each type of type graph calculates the incidents uniquely and exports the summarized data to a different table in the Selection.MDB that is located in the [project workspace](#).



Selection.MDB contains the sources for the graphs.

The Selection.MDB is automatically created if it is not present in the project workspace. If the summarize table already exists in the Selection.MDB it is deleted and replaced.

The table in the Selection.MDB is then used with the graph template that is stored in the \Desktop\Graphs\ folder in the OmegaGIS installation directory.

For more graph options, right-click the title bar of the graph window.



Layout Metadata Editor

Availability by Extension

CrimeView	FireView	School Planner
Layout Metadata Editor	Layout Metadata Editor	Layout Metadata Editor

The Layout Metadata Editor adds information to the layout about the last OmegaGIS routine run. This tool will only be available when the Layout View is visible. To make the Layout View active, select 'Layout View' from the 'View' menu.

[Inputting Information](#)

[Advanced and Preview Buttons](#)

[Generating Output](#)



Select the information from the last OmegaGIS Routine completed to add to the layout.

Attachment A**Inputting Information**

To add information to the layout, select the desired checkboxes and edit the text, if needed. The text is only editable if the checkbox has been selected. There are three subdivisions of information that can be included in the output. The text between each of these divisions is separated with a light cyan (red=140 green=178 blue=210) dashed line.

Disclaimer

This text is inserted as the last division of text in the output text box. The default disclaimer text can be updated on the 'General' category of the [OmegaGIS Setup](#). The text is limited to 255 characters.

Title Information

This information is added to the layout as the first division of the output text as the title. This information is stored in the OmegaGIS routine metadata that is saved when a routine is created. If the routine metadata cannot be found, this information will not be available to add to the layout.

- **Name**

This setting will be displayed as a medium cyan (red=70 green=130 blue=180) color. The maximum length of text inserted into this box is 100 characters. The default for this text box is the name of the last OmegaGIS routine run, for example, 'Near a Feature'.

- **Date**

This setting will be displayed in black text and can be a maximum of 30 characters long. The default for this text box is the date that the last OmegaGIS routine was run. The maximum number of characters that can be typed into this text box is 30.

Last Routine Information

This information is added to the middle division of the output text. Each setting in this division will be prefixed by the label describing the text in the each text box. For instance, the Layers: setting will include not only the text inputted in the text box but also the word 'Layers: ' as a prefix. All of the settings in this section produce black text. This information is stored in the OmegaGIS routine metadata that is saved when a routine is created. If the routine metadata cannot be found, this information will not be available to add to the layout.

- **Layers:**

Attachment A

This text box by default contains the list of layer(s) separated by commas used in the last OmegaGIS routine run. This text box can accept characters up to 255.

- **Query:**

This text box includes the query used during the last OmegaGIS routine. The query that is displayed is the query that is shown in the 'Edit Query' box on the **What?** tab of OmegaGIS routines. This box can be up to 500 characters in length.

- **Dates:**

This text box shows any date queries that were specified on the **When?** tab of the last run OmegaGIS routine. The beginning and end dates are separated by a dash. The maximum number of characters that can be entered into this text box is 50.

- **Times:**

This text box shows any date queries that were specified on the **When?** tab of the last run OmegaGIS routine. The beginning and end times are separated by a dash. The box can be up to 50 characters in length.

- **Days:**

This text box shows any day queries that were specified on the **When?** tab of the last run OmegaGIS routine. Each day is separated by semicolons. The maximum length of text inserted into this box is 50 characters.

Advanced and Preview Buttons

Advanced Properties

- **Text Box Placement**

By default, the text box is added to the lower right corner of the layout. Select another location from the drop-down list, if desired.

Attachment A

- **Text Box Width**

By default, the text box is 46 characters wide. This means that sentences that contain more than 46 characters will wrap to another line. Enter a different number to change the width of the text box. The width must be between 10 and 100 characters.

- **Text Box Border**

Checking this setting adds a border around the text. Otherwise, only the text is added to the layout. By default, a border is created around the text.

- **Show disclaimer in italics**

Checking this setting displays only the disclaimer text in italics in the layout. Otherwise the text is shown as regular text. This setting by default puts the disclaimer in italics.

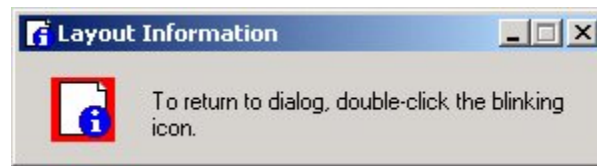
**Preview**

When the 'Preview' button is clicked the following events will occur:

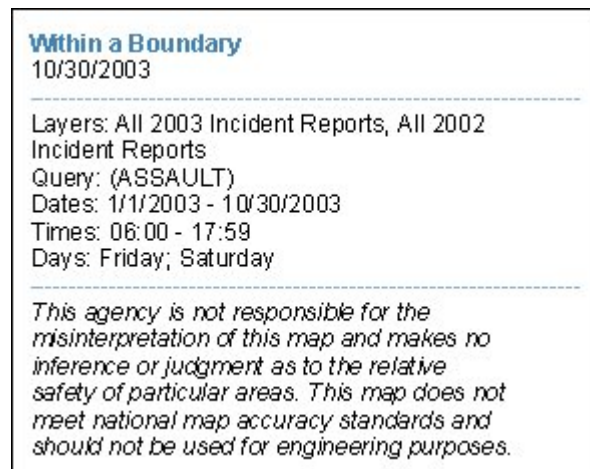
- The text based on the current settings will be added to the layout.

Attachment A

- The Layout Information dialog will shrink and the icon will blink. Click the blinking icon to restore the Layout Metadata Editor dialog.

**Generating Output**

Clicking 'OK' will add the specified text to the layout. Each time the 'OK' or 'Preview' button is selected any existing text generated by this tool will be removed.

**Editing after clicking 'OK'**

To edit the text you specify with this dialog, either double-click it with the Select Graphics tool (the black pointer), or click the Text tool (the black A) and then click inside the text on the map and make your edits. If a border is included around the text box, use the 'Ungroup' option on the Drawing toolbar to be able to edit the text.

The text in this tool is drawn using its symbol settings. In some cases these symbol settings are overridden for particular portions of the text by inserting ArcMap text formatting tags. This lets you create mixed-format text where, for example, one word in a sentence is underlined. The ArcMap text formatting tags follow XML syntax rules. Each start tag must be accompanied by an end tag. Tags can be nested, but you must close the inner tag before closing an outer tag. The case of tag

Attachment A

pairs must match exactly. Tag attributes may be surrounded by either single or double quotes. '&' and '<' are special characters and are not valid in your text if formatting tags are used. Use the equivalent character codes & and <. A list of common XML tags are shown below.

Font:	<FNT name="Arial" size="18">My text</FNT>
Color:	<CLR red="255" green="255" blue="255">My text</CLR> <CLR cyan="100" magenta="100" yellow="100" black="100">My text</CLR>
Bold:	<BOL>My text</BOL>
Italic:	<ITA>My text</ITA>
Underline:	<UND>My text</UND>
All caps:	<ACP>My text</ACP>
Small caps:	<SCP>My text</SCP>
Superscript	^{My text}
Subscript:	_{My text}
Character spacing (%):	<CHR spacing="25">My text</CHR>
Word spacing (%):	<WRD spacing="150">My text</WRD>
Leading (pts):	<LIN leading="12">My text</LIN>

For more information about formatting text see ArcGIS Desktop Help.

Remove Layout Elements

Availability by Extension

CrimeView	FireView	School Planner
Remove Layout Elements	Remove Layout Elements	Remove Layout Elements

In ArcMap, the layout contains all of the elements of a map. These map elements may include a title, agency logo, legend, north arrow, scale bar and geographic layers.

Attachment A

When creating a [new layout](#), it may be necessary to remove these map elements and start again. The Remove Layout Elements tool removes all map elements from the layout. The only map elements that are not removed are the data frames and any neatlines around a data frame.

The Remove Layout Elements tool is available from the pull-down menu of an Omega GIS toolbar, such as CrimeView. The tool is only enabled when the layout is the active view in ArcMap. When the tool is selected, one is prompted as to whether or not to remove all the map elements in the layout.

Create Grid

Availability by Extension

CrimeView	FireView	School Planner
Create Grid	Create Grid	Not Available

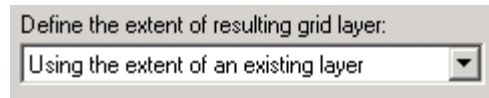
The Create Grid tool is used for the creation of polygon rectangular grid layers in a personal Geodatabase. To use the tool, the ArcMap document must be saved.

1. Select the extent for the polygon grid layer from the pulldown list, the options include:

- Using the extent of an existing layer.

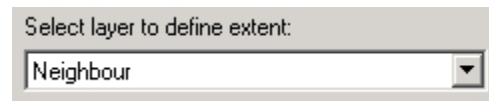
Attachment A

- Using the extent of the selected features.
- Using selected rectangle graphic.



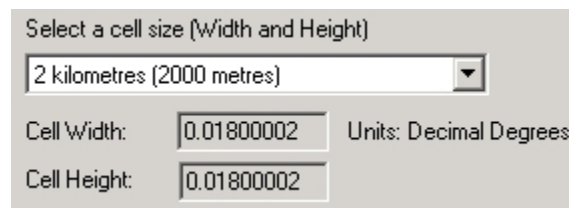
Define the extent of resulting grid layer:
Using the extent of an existing layer

2. From the pulldown list of valid layers in the active data frame, select the layer to use as the extent of the grid layer. This list is disabled when using a rectangle graphic.



Select layer to define extent:
Neighbour

3. Select a pre-defined cell size of the grid from the pulldown list. Below the list will be the width and height of the grid cell in map units. The width and height of the grid cell can only be edited when the cell size of 'user-defined' is selected.



Select a cell size (Width and Height)
2 kilometres (2000 metres)
Cell Width: 0.01800002 Units: Decimal Degrees
Cell Height: 0.01800002

4. Provide a name for the new grid layer and the location of the personal geodatabase (pGDB). By default, the tool will generate the layer in the Grids.mdb in Grid folder located in the OmegaGIS project directory.

If the pGDB does not exist, it will be created. There must not be a layer within the pGDB that already has the same name of the new grid layer.

Attachment A

5. Click the **Create Grid** button to generate the new grid layer.

About Demographic Viewer

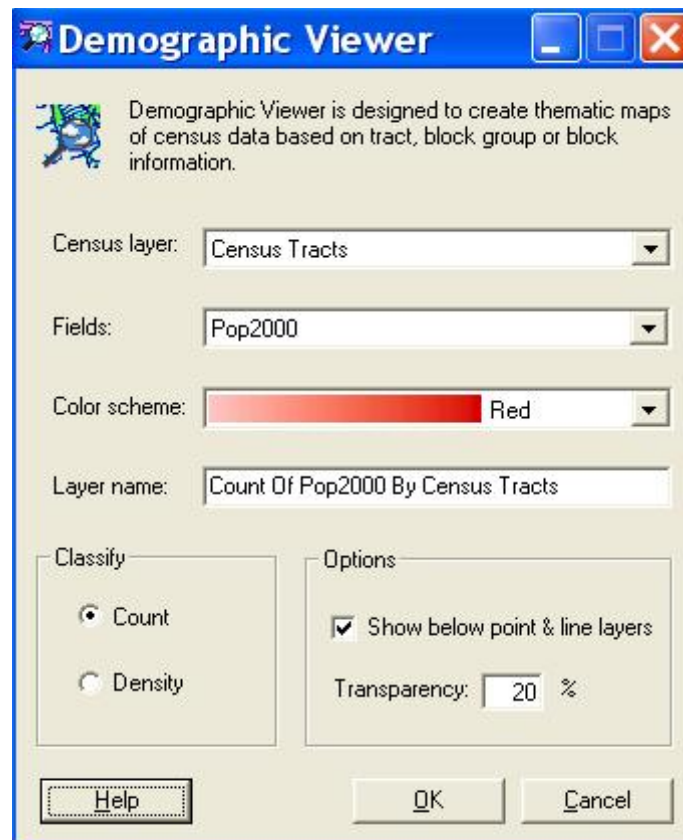
Availability by Extension

CrimeView	FireView	School Planner
Demographic Viewer	Demographic Viewer	Demographic Viewer

Demographic Viewer is designed to quickly display census data as thematic map layers in ArcGIS. The tool displays either population count or population density based on a demographic attribute selected from the census layer.

Demographic Viewer was first designed to be used with the data format of Tiger Line/Census files available from ESRI at www.esri.com. Demographic data used with this utility can be downloaded and formatted according to the specifications outlined in the [Accessing Demographic Data](#) document. The [Demographic Data Loader](#), available in ArcCatalog, provides an easy method for preparing the demographic data provided by ESRI for the Demographic Viewer. Census information outside of that provided by the U.S. Bureau of the Census, can be used as well, but must be formatted appropriately in order to be used with the utility.

To access Demographic Viewer, open up the Tools menu from the ArcMap toolbar, and select extensions. Select the OmegaTools extension to ensure access to the tools. Click on 'Customize' from the 'Tools' menu, and again select the OmegaTools extension to open the new extension as a toolbar.

Attachment A

Creating Census Data

Census data can provide an excellent source of additional information when analyzing crime statistics. Incorporating census data into an analysis, can lead to a better understanding of how and why crimes occur, while determining resources necessary for crime prevention.

As a part of OmegaGIS, Demographic Viewer and Crime Rate Generator enable the incorporation of census information into viewing and analyzing crime data. Both utilities were initially designed to be based on standardized census information available from the ESRI website, under the Data section of their main webpage (www.esri.com). However, it is possible to use other sources of census information with these tools provided the data is formatted appropriately.

[Description of Source Data](#)

[Accessing Census Data](#)

Description of Source Data

The U.S. Bureau of the Census provides census data that is distributed by ESRI. The data is created at three resolutions, census blocks, census block groups and census tracts and is available nationwide. Detailed metadata about the data can be acquired from both the ESRI website and the U.S. Bureau of the Census. <http://www.census.gov/>

Census Tracts

Census Tracts form the largest of the three boundary types. The boundaries tend to be relatively stable, covering subdivisions of a county or equivalent entity. Census tracts represent a continuous land area, where all parts are internally accessible by road. The total area and population of a county must be covered by the Census Tracts.

Census Block Groups

Census Block Groups are subdivisions of Census Tracts. Their boundaries always follow Census Tract boundaries, and generally are delineated by visible and identifiable features such as rivers, roads or power lines. Each Census Tract comprises between one and nine Census Block Groups. Block Groups form a compact and contiguous group of Census Blocks, and provide a summary of block information.

Census Blocks

Blocks are the smallest geographic units for which demographic information is compiled by the U.S. Bureau of the Census. In many cases, Census Blocks follow individual city blocks and are bounded by streets. There are cases however, especially in rural areas where blocks may span many miles, and where their boundaries do not relate to streets.

Data Format

The data provided is distributed as a shapefile and an associated flat file. The shapefile houses the census geographic boundaries. When unzipped, the shapefile consists of the three standard files that make up a shapefile on disk; .shp, .shx and .dbf. The flat file is distributed in .dbf format and includes all of the population statistics compiled by the U.S. Bureau of the Census for each polygon in the shapefile.

Attachment A

Do not alter the names of the files if planning to use the Demographic Data Loader to create the census data. An option exists in the Demographic Data Loader utility to automatically select all of the census files for data compilation, which then updates the various text boxes on the form. This option may save some time in browsing for each of the files, but does not automatically recognize the files if the names have been changed.

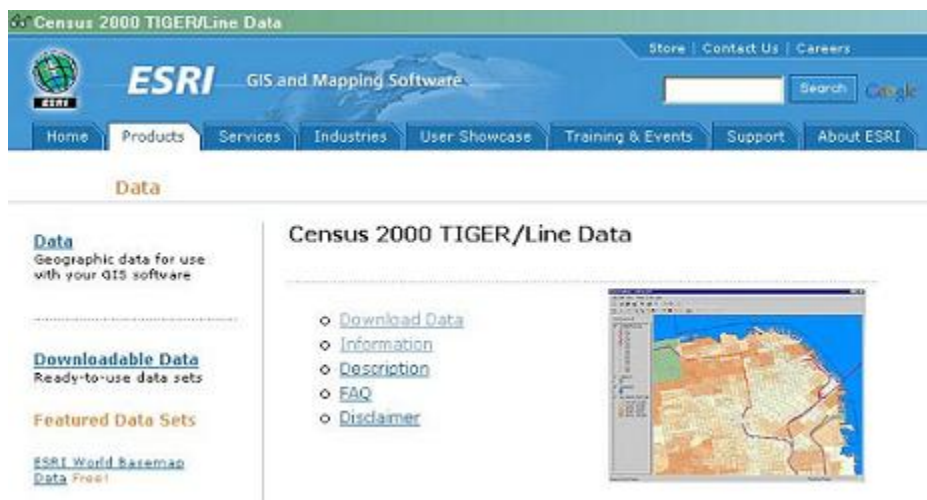
Accessing Census Data

Census information used by OmegaGIS is available through the ESRI website. The following steps outline the method for accessing and downloading the necessary files:

1. Go to the following URL:

http://www.esri.com/data/download/census2000_tigerline/index.html

2. Click on the Download Data link.

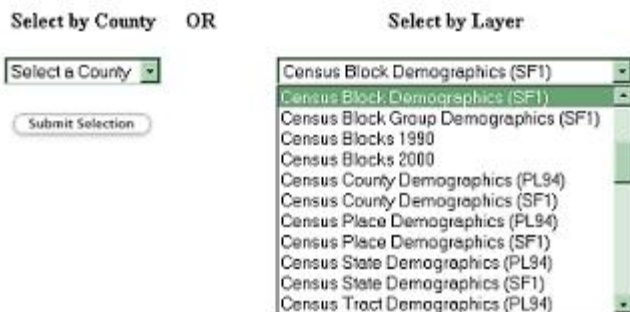


Attachment A

3. In the map, click on the State for which you want to extract data.



4. Select the County you need data for and click Submit Selection.



5. From the Available data layers, select the following three (3) layers to download (these are the boundaries in shapefile format):

- Block Groups 2000
- Census Blocks 2000
- Census Tracts 2000

6. From the Available Statewide Layers, select the following three (3) layers to download:

Attachment A

- Census Block Demographics (SF1)
- Census Block Group Demographics (SF1)
- Census Tract Demographics (SF1)

If the Census Block Demographics are not available with a check box, you may need to download the entire state separately. There may be a link to do this on this same page. Omega has already downloaded all of the block data for California.

7. Click Proceed To Download.

8. When your file is ready, click Download File.

9. Save the file in your \temp folder and extract all of the data layers into their own folder on your hard drive to start processing for use.

10. Load the data using the [Demographic Data Loader](#).

Using the Demographic Viewer

The dialog provided with Demographic Viewer is relatively simple and intuitive to use, however it is important to keep in mind the way in which data is made available to the tool. The following topics describe the way in which data is loaded into the Demographic Viewer. The sections also outline how to use this data to create new demographic layers.

[Census Layer](#)

[Fields](#)

[Count and Density](#)

Attachment A

[Below Point and Line Layers](#)

[Transparency](#)

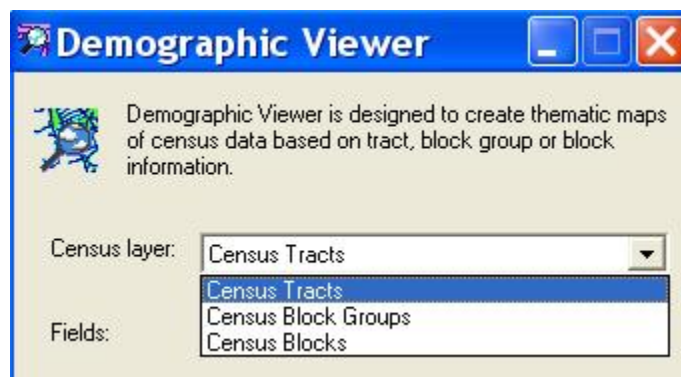
[Resultant Census Layer](#)

Census Layer

When the dialog is loaded, the table of contents is searched for layers containing a registered type of 'Census_Block', 'Census_Blockgroup' or 'Census_Tract'. When compiling the data using the [Demographic Data Loader](#) in ArcCatalog, the registered type is set automatically. If the data is not created with the Demographic Data Loader, the [OmegaGIS Metadata Editor](#) can be used to set the layer's registered type to 'Census_Tract', 'Census_Blockgroup' or 'Census_Block'.

Once the registered type is identified as one of the 'census' types above, the layer's data source is searched. If the data source is valid, the layer has met two of the three requirements necessary to add the layer to the list box. The final qualifier is that the layer must have a geometry type of 'Polygon'.

If no layers are found in the table of contents meeting these requirements, a warning message is issued to indicate that the Demographic Viewer is unavailable. At least one Census layer must be found in the table of contents to enable the tool.



Fields

Attachment A

The Fields list box lists the attributes found in the census layer selected in the 'Census Layer' list box. The fields are added to the field list box if they meet the following requirements:

- The field is not a length or area field.
- The field is numeric.

The census data provided by ESRI includes the following fields which are automatically omitted from the field list as they cannot be summarized:

- Med_age Median Age
- Med_age_M Median Age Male
- Med_age_F Median Age Female
- Avg_hh_sz Average household size
- Avg_fam_sz Average family size
- Hse_Units Household units
- Rural
- Urban
- Vacant
- ID

Count and Density

Count and Density options are available to display the resulting census data. The count option simply displays the population for each polygon in the census layer. The population data rendered depends on the field that is selected in the layer.

Attachment A

To create the thematic layer, the data is divided into five classes based on the Jenks Natural Breaks classification method. Natural Breaks determines the class intervals by grouping similar values into the same class. Each class is then assigned a color based on the color ramp selected in the Viewer. The color ramps available are those found in the [OmegaGIS.STYLE](#) file.

The Density option displays the demographic data in exactly the same manner but normalizes the data by dividing the population count by the area of the polygon. The area of each polygon is calculated in square miles or square kilometers depending on the OmegaGIS Setup setting that sets the units of measure to either 'English' or 'Metric'.

If the census layer is in a projected coordinate system, the area calculation is straight forward. However if the layer is in a geographic projection, the area cannot be calculated directly. The results are dependent on the latitude of the study area due to the nature of geographic projections. In order to accommodate these calculations, if a geographic projection is encountered, the geometry of the census layer is projected temporarily to the coordinate system 'North America Lambert'.



Population Count

Population Density

Display Below Point and Line Layers

Attachment A

The default position in the table of contents for new layers is at the very top of the stack. Placing a layer here, may obstruct features in layers below. The Display Below Point and Line Layers places the new census layer below any layers with a geometry type of point or polyline, so that these features are not blocked.

Transparency

Setting the transparency on a layer is used to both view the layer, while also being able to see the features of underlying layers. Transparency ranges from 0 to 100, where 100 is completely transparent and 0 is opaque.

Resultant Census Layer

The census layer created by the Demographic Viewer is placed in the map table of contents. It adopts the coordinate system of the source layer on which it is based. The new layer's source data is located in the [project workspace](#) \census folder within a database called Omega_DemoViewer.mdb. The new feature class is always called census_*. Where * is a numeric value used to create unique feature class names. When the layer is no longer referenced by the ArcMap document, it is removed automatically during [Project Cleanup](#).

Omega Tab

Availability by Extension

CrimeView	FireView	School Planner
Omega Tab	Omega Tab	Omega Tab

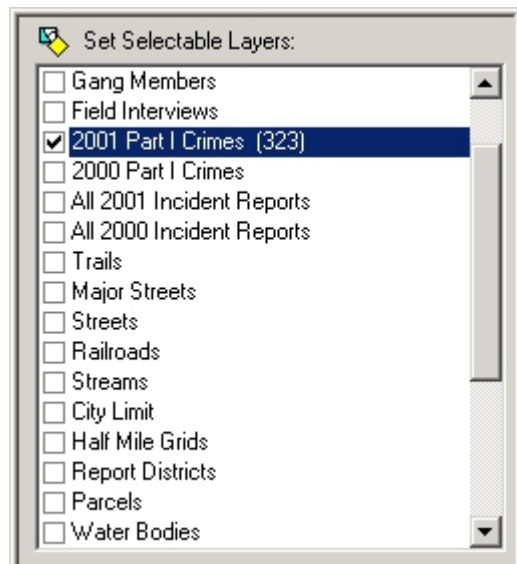
Attachment A


ArcMap contains two tabs in the table of contents: the Display and Source tab. When an OmegaGIS extension is enabled such as CrimeView, FireView or School Planner, the Omega tab is added to ArcMap. The Omega tab is used to set which layers are selectable and to view layer metadata.

To prevent the Omega tab from being added to ArcMap automatically when an OmegaGIS extension is enabled, un-check the setting in the [OmegaGIS Setup](#) dialog. The change occurs when ArcMap is reopened.

Selectable Layers

The list at the top of the Omega tab contains all of the feature layers in the active data frame that are selectable and are valid. Layers are not valid if the reference data is missing (layer has a red exclamation mark in the ArcMap Display tab).



Layers that have a check mark in front of their name are selectable. The Select Feature tool  in ArcMap only selects features in those layers that have been set to be selectable.

After the layer name in brackets is the number of selected features for that layer. This number is updated when there is a change in the selection in the active data frame. This functionality can be disabled by a setting in the [OmegaGIS Setup](#) dialog.

Metadata

The metadata for the selected item in the Selectable Layers list is displayed at the bottom of the tab.

Attachment A

The metadata displayed includes:

Type: Layer type which is set in the [OmegaGIS Metadata Editor](#).

Default Field: Name of the field that is automatically selected in OmegaGIS routines. The default field is set with the [OmegaGIS Metadata Editor](#).

Query Groups: [Saved query](#) group to which the layer is registered. The OmegaGIS Metadata Editor is used to register the saved query groups.

Reports: Name of the [Crystal Reports](#) registered to the layer. Reports are registered to a layer with the OmegaGIS Metadata Editor.

Updated: Date (yyyy-mm-dd) That the layer was last updated by the Omega Import Wizard.

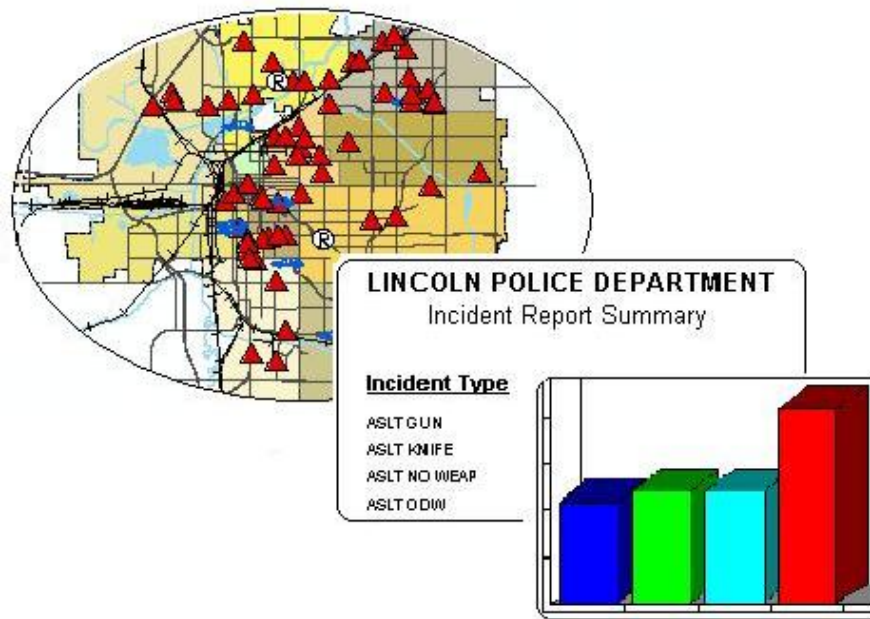
If an item outlined above is missing, then there is no information for the layer.

Tip

- Limit the number of selectable layers to improve performance while using the Select Feature tool. ArcMap must perform a spatial query on each layer that is selectable when using the tool.
- For metadata information about the import process, use the OmegaGIS stylesheet in ArcCatalog.

About Cyclical Reports

Cyclical Reports are created in order to store the parameters of common queries and density routines so that they may be run repeatedly and without spending time resetting the parameters. A query or density map created with either of the OmegaGIS [Query](#) or [Density](#) routines can be stored as a Cyclical Report. When run, the Cyclical Report recreates the query or density request, and produces the results geographically as a map layer, as well as opening any reports or graphs that have been saved as a part of the Cyclical Report.



Cyclical Reports Setup

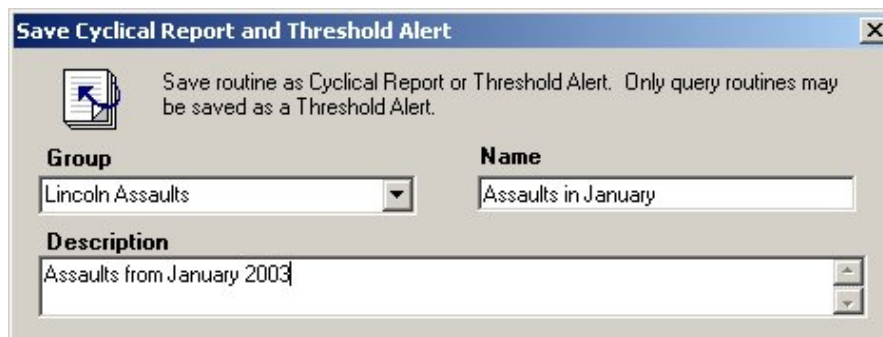
Creating a Cyclical Report

Cyclical Reports are based on Query and Density routines. **It is extremely important to note that when designing a Cyclical Report, the date range must be identified using the 'Previous' control on the When tab of the dialogs. Interactively setting the date range using the calendars will result in incorrect results when the Cyclical Report is run.**

Attachment A

Once a Query or Density routine is set up, saving the routine as a Cyclical Report can be accomplished from the Query routine Summary Dialog available in OmegaGIS. The Summary Dialog appears after the options of a query or density routine are set, and the Finish button is clicked. If the Summary Dialog does not appear before the routine finishes running, check [OmegaGIS Setup](#) to ensure that the 'Display the routine summary...' option is checked under the Queries category.

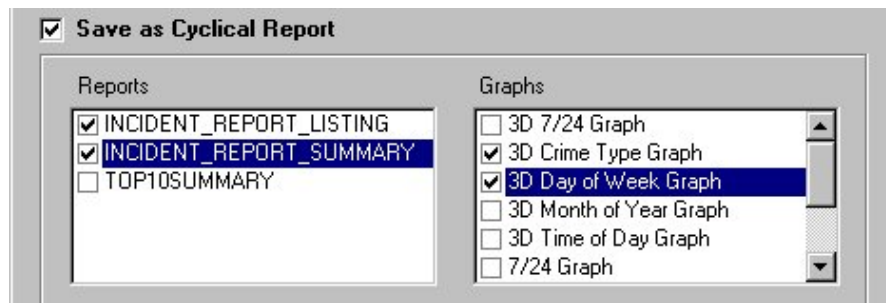
To open the Cyclical Report menu, click on the Save button from the Summary Dialog.



When the new menu opens, a Group must either be selected from the drop-down list, or a new Group must be entered into the text box. The Group identifies to which collection the particular Cyclical Report belongs. The Group allows Cyclical Reports to be organized into different categories. Sub-dividing the reports creates a more manageable project as the number of reports increases.

A Name must be entered for each Cyclical Report, and must be unique to the Group to which it belongs. If a duplicate name is entered, a message box issues a warning. The Description field is not required, however adding detail to a Cyclical Report can increase the manageability of the project as the number of reports grows.

When the Group, Name and Description are determined, check the 'Save as Cyclical Report' to save the query or density routine as a Cyclical Report. In addition to saving the query or density routine that will run using the parameters specified on the query or density dialog, the Cyclical Report can save a number of reports or graphs that will be generated the next time the report is run. These reports can be sent with a Threshold Alert as PDF files when the alerts are emailed.

Attachment A

Reports

The list presented in the Reports window is a compilation of all of the reports that have already been registered to the Query layer. For instance, during the creation of the query or density routine, the Query Layer '2001 Part I Crimes' is selected. From the Query Summary dialog, the Save button is clicked to open the 'Save as Cyclical Report...' dialog. The reports that appear in the Cyclical Report window consist of those reports that were registered to this layer using the OmegaGIS [Metadata Editor](#).

Any report registered to the Query layer for a Query routine is shown in the Report list. For Density routines however, the report list is disabled for both [Density](#) and [Hot Spot](#) maps. For [Repeat Calls](#), the Repeat Calls report may show up in the list if it has been registered to the query layer using the OmegaGIS Metadata Editor.

Crystal Reports is used by the Omega Project Manager to create the standard reports that are issued with each OmegaGIS project. Additional reports can always be created and customized, and will appear in the report list box if they are also registered to the appropriate layers using the OmegaGIS Metadata Editor. In addition, it is important to ensure that OmegaGIS can find all of the reports necessary for the project. Use the Database category in [OmegaGIS Setup](#) to set the locations on disk that are searched for reports.

Graphs

The list presented in the Graphs window represents the standard graphs that are delivered with OmegaGIS. The graphs that show up in this list are based on whether OmegaGIS Date, Time and Day of Week fields are available in the layer that is being queried. If multiple OmegaGIS fields exist within the layer, the default OmegaGIS field is selected for calculations. The default OmegaGIS field can be set using the OmegaGIS Metadata Editor.

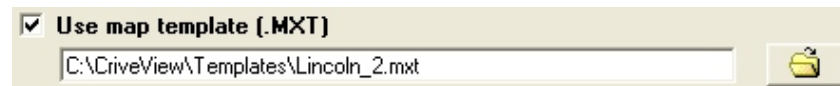
Attachment A

Any standard graph that meets the OmegaGIS field requirement for a [Query layer](#) based on the Query routine will show up in the list. However, the Graph list will be disabled for any Query layer created using the Density, Hotspot, or Repeat Calls routines.

Map Template

[Map templates](#) are used to define how the map elements in the layout appear. Map elements include a title, agency logo, legend, north arrow and scale bar. Check the Use Map Template checkbox and then click the browse button to navigate to an existing map template (.MXT).

With the release of ArcGIS 10, creating map templates is no longer supported by ESRI. Existing map templates may be used to create Cyclical Reports, however, no new templates may be created.



When a map template is selected, the following items are checked:

- The MXT contains a layout.
- The MXT contains the same number of data frames as the current ArcMap document.

When editing a Cyclical Report the map template is verified and if there is a problem a red exclamation mark is visible beside the path to the template. The following checks are made on the template:

- The MXT file can be located on disk.
- The MXT contains a layout.
- The MXT contains the same number of data frames as the current ArcMap document.



Attachment A

When the Cyclical Report is run, the same validation of the map template occurs. If the template is valid, the layout is made the active view in ArcMap and the template is loaded. If the map template is not valid, the template is not used and there is no warning provided.

Editing Cyclical Reports

On the 'Save Cyclical Report...' dialog, an Edit button is visible, however it remains disabled. The Edit button references the actual Query or Density routine used to create the Cyclical Report. Since it is possible to edit the query by simply canceling the dialog, and then clicking the back button on the Summary Dialog, this feature is unnecessary and is disabled.

The Edit button is enabled when the 'Save Cyclical Report...' form is opened from the 'Cyclical Report' dialog. In this case, you cannot backtrack to the Query or Density dialog directly, so the Edit button is necessary to edit the parameters of the initial Query or Density routine.

The Cyclical Reports Database

The database housing all of the information important to Cyclical Reports is called Threshold_Alert.mdb and is found in the [project workspace](#). In [pre-Service Pack 2](#) versions of OmegaGIS, the Threshold_Alert database was referred to as the Cyclical.mdb database as it stored files pertaining to cyclical reports only. However, to accommodate the new functionality of Threshold Alerts, this database has been updated to include the data pertinent Threshold Alerts as well.

As a consequence of these updates, any projects created with previous versions of OmegaGIS software in the ArcGIS environment, must replace the cyclical.mdb database with the new threshold_alert.mdb database. Any cyclical reports created in the old environment must be recreated in the new environment, in order to save them in the format required.

Running a Cyclical Report

Attachment A

Opening a Cyclical Report

Once created, a Cyclical Report can be opened at any time by accessing the report from the 'Cyclical Reports' Button of the Main Menu. If there are no Cyclical Reports in the project, a warning message is issued and Cyclical Reports is unavailable.

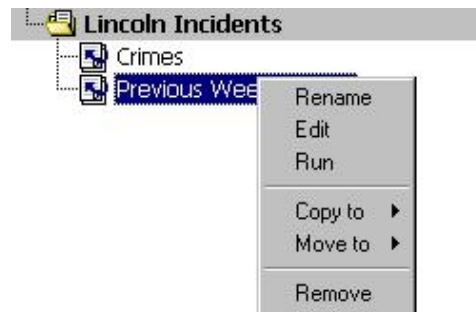


Cyclical Reports Dialog

When the Cyclical Reports dialog is opened, any of the reports created previously can be viewed and run again. On the left hand side of the dialog is a listing of the Groups, and the Cyclical Reports contained within those Groups. To select a Cyclical Report, click on the report name in the list. Once a report is selected, the right hand side of the dialog is updated with a general description.

Attachment A**Cyclical Report Options**

Each Cyclical Report can be run simply by clicking on the Run button at the bottom of the dialog. However, by right-clicking on the Cyclical Report name, a number of additional options become available.



The following options are provided on the pop-up menu when the Cyclical Report is selected:

Rename

Create a new name for the Cyclical Report.

Attachment A**Edit**

The Edit menu item opens up the 'Save Cyclical Report...' dialog. In this dialog, the Cyclical Report name and description may be modified, as well as the reports and graphs that are saved as components of the cyclical report.

Run

Run the selected Cyclical Report.

Copy To

Copy the selected Cyclical Report to a different Group.

Move To

Move the selected Cyclical Report to a different Group.

Remove

Delete the Cyclical Report.

About Threshold Alert

Threshold Alert is a versatile utility that can be used to notify decision makers when incidents exceed an acceptable threshold. The distribution of information is made immediate, by setting up email addresses in advance. The results of OmegaGIS queries can then be automatically made available to the appropriate personnel when a critical number of events have occurred.

Three important steps must be accomplished in order to create and distribute threshold alerts. The first step is to identify what type of threshold alerts are required. Threshold Alert is similar to [Cyclical Reports](#) and is available to any of the [Query](#) routines. Once the alerts required are created, the next step is to identify who will receive the information. During this stage, the email server and email addresses of the recipients must be identified. Finally, each threshold alert must be assigned to the appropriate personnel. When these steps are complete, it is possible to automate the process.

Attachment A

Understanding Threshold Alerts

In setting up a system of Threshold Alerts, it is important to understand the process whereby information is retrieved from the source database, and processed for analysis. Typically, two streams of data exist, Computer Aided Dispatch (CAD) and Records Management System (RMS). CAD information is immediate, as it is collected as incidents are called in, whereas RMS data is filtered from the CAD calls, and is only as current as the data processing to enter new records into the system.

If for example, it takes three weeks to enter records from the initial CAD database into the RMS system, sending a Threshold Alert based on the RMS records is not beneficial to assist in an immediate response to specific incidents. It is important to understand the flow of information before creating a series of threshold alerts.

Threshold Alert Results

Threshold Alerts may be emailed as both a map, and a series of Crystal Reports. A map template may be used in order to include map surround elements. The format of the map that is emailed depends on whether the ArcMap project was last saved in a data view or layout view. If ArcMap was saved in 'layout view', the map can include any of the map surround elements included with the page; such as a legend or disclaimer. Any reports generated by the cyclical report on which the threshold alert is based, can be sent as attachments to the email as PDF files. The limitation on the number of reports that can be sent is associated with the file email attachment file size limitation.



Threshold Alert Setup

[Creating a Threshold Alert](#)

[Setting Threshold Alert Email Servers](#)

[Setting Threshold Alert Emails](#)

[Managing the Threshold Alert Database](#)

[Limiting Alert Notifications](#)

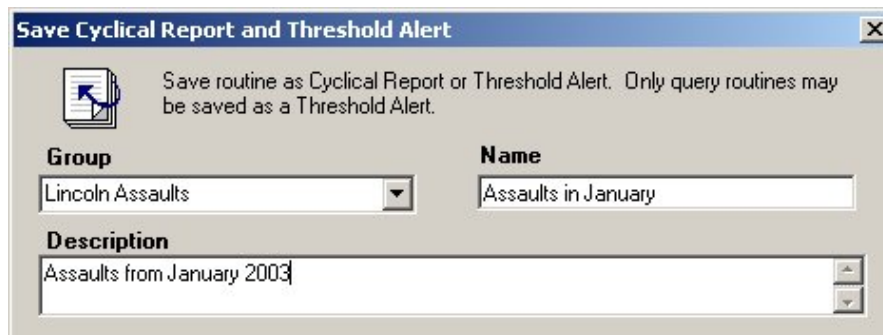
Attachment A

Creating a Threshold Alert

Threshold Alerts are based on Query Routines. **It is extremely important to note that when setting a date range for a Threshold Alert, the 'Previous' control on the date-time dialog must be used to select the beginning and end dates. Interactively setting the dates using the calendars will result in incorrect results when the Threshold Alert is run.**

Threshold Alerts are accessed from the [Query routine](#) Summary Dialog available in OmegaGIS. The Summary Dialog appears after the options of a query are set, and the Finish button is clicked. If the Summary Dialog does not appear before the routine finishes running, check [Omega Setup](#) to ensure that the 'Display the routine summary...' option is checked under the Queries category.

To open the Threshold Alert form, click on the Save button from the Summary Dialog.



Save Cyclical Report and Threshold Alert

Save routine as Cyclical Report or Threshold Alert. Only query routines may be saved as a Threshold Alert.

Group
Lincoln Assaults

Name
Assaults in January

Description
Assaults from January 2003

When the new dialog opens, a Group must either be selected from the drop-down list, or a new Group must be entered into the text box. The Group identifies to which collection the particular Threshold Alert belongs. The Group becomes important when designing email notifications, as all of the threshold alerts belonging to the Group are mailed as a collection to the designated personnel.

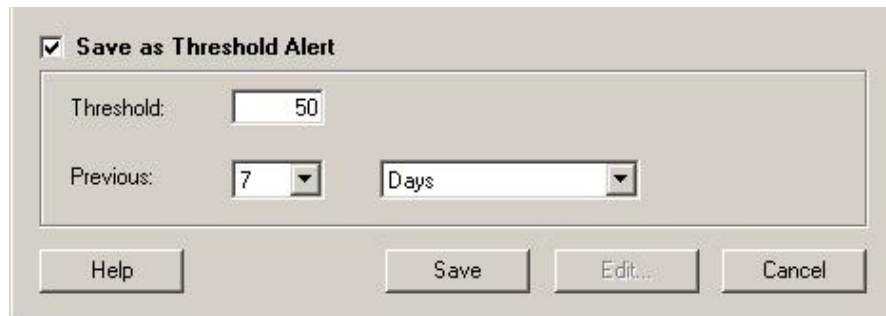
An additional note about Groups is important when using Threshold Alerts and Cyclical Reports. Both routines use the concept of a 'Group' in order to categorize reports and alerts. This means that the Group list will contain Group names for both Cyclical Reports and Threshold Alerts.

A Name must be entered for each threshold alert, and must be unique to the group to which it belongs. If a

Attachment A

duplicate name is entered, a message box issues a warning. The Description field is not required, however adding detail to an alert can increase the manageability of the project as the number of alerts grows.

When the Group, Name and Description are determined, check the 'Save as Threshold Alert' to save the query as an alert. The Threshold refers to the number of incidents that must be exceeded in order to produce an alert. Using the Previous text boxes, a specific duration can be set to search for the incidents in question.



Through this menu, an Edit button is visible, however it remains disabled. The Edit button references the actual query used to create the threshold alert. Since it is possible to edit the query by simply canceling the dialog, and then clicking the back button on the Summary Dialog, this feature is unnecessary from this menu and is disabled. The Edit button becomes enabled when accessing this menu from the [Threshold Alerts and Notifications dialog](#).

Map Template

[Map templates](#) are used to define how the map elements in the layout appear. Map elements include a title, agency logo, legend, north arrow and scale bar. Check the Use Map Template checkbox and then click the browse button to navigate to an existing map template (.MXT).

With the release of ArcGIS 10, creating map templates is no longer supported by ESRI. Existing map templates may be used to create Threshold Alerts, however, no new templates may be created.



Attachment A

When a map template is selected, the following items are checked:

- The MXT contains a layout.
- The MXT contains the same number of data frames as the current ArcMap document.

When editing a Cyclical Report the map template is verified and if there is a problem a red exclamation mark is visible beside the path to the template. The following checks are made on the template:

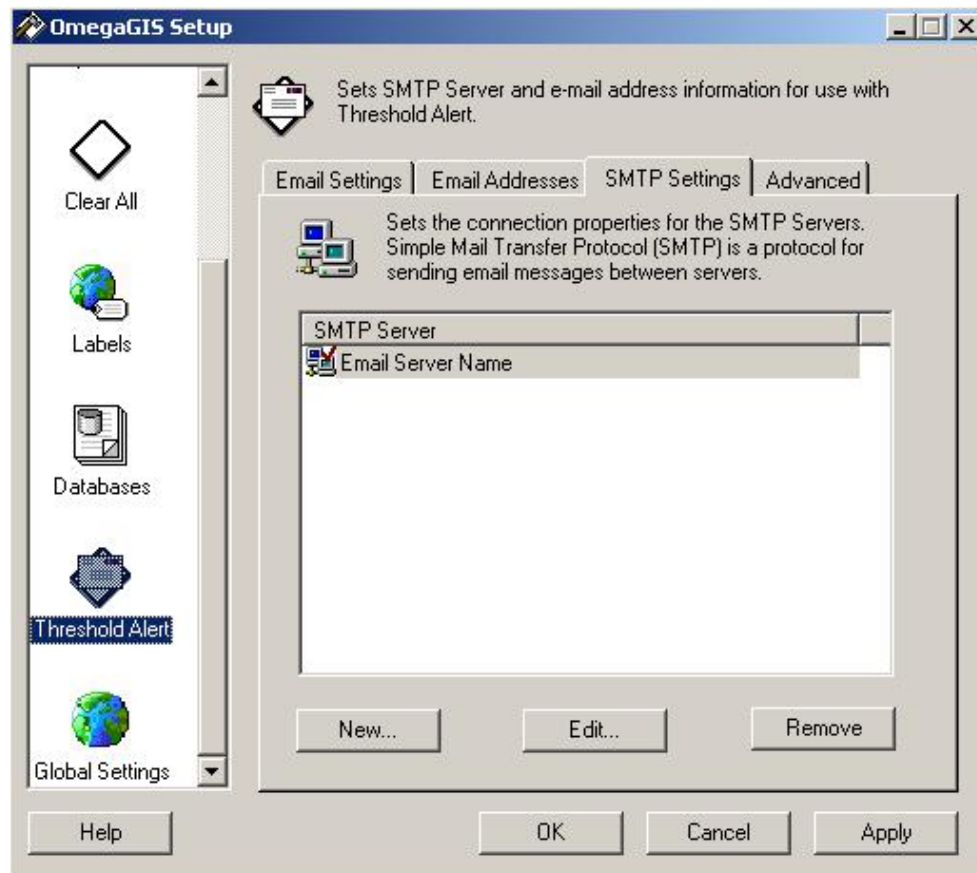
- The MXT file can be located on disk.
- The MXT contains a layout.
- The MXT contains the same number of data frames as the current ArcMap document.



When the Cyclical Report is run, the same validation of the map template occurs. If the template is valid, the layout is made the active view in ArcMap and the template is loaded. If the map template is not valid, the template is not used and there is no warning provided.

Setting Threshold Alert Email Servers

In order to send Threshold Alerts to the appropriate personnel, an email server must first be selected, and the addresses of those receiving Threshold Alerts must be entered. To set up these options, open OmegaGIS Setup and click on the Threshold Alert Icon.

Attachment A

The first step in setting up the Email Server information is to research the fully qualified domain name(s) or IP address(es) of the SMTP Server at your site. Contact your system administrator for this information. The SMTP Server must be accessible from the computer where the Threshold Alerts are to be run. URL addresses, such as <http://mail.yourdomain.com> are not supported.

When the name(s) or IP address(es) are acquired, they can be entered into a list using the New button. Clicking on the New button opens a dialog which provides a text box for either the Name or the IP address. This information can be entered manually or browsed from a list of servers on your network.



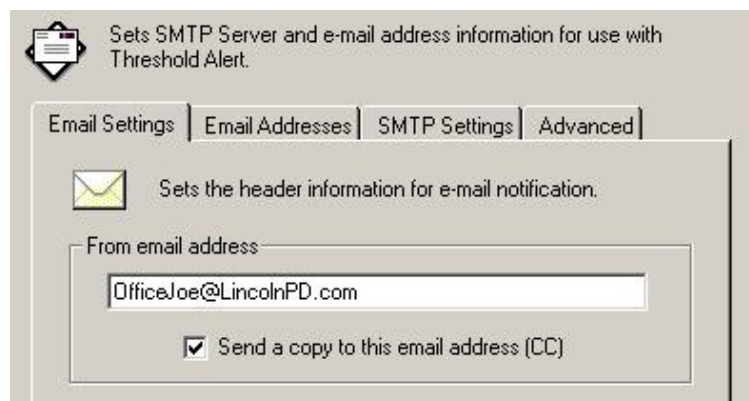
Attachment A

Selecting the checkbox 'Use this server as the default' automatically assigns the server to any email address entered after the default server is set. The default server is identified by a red checkmark within the server icon.

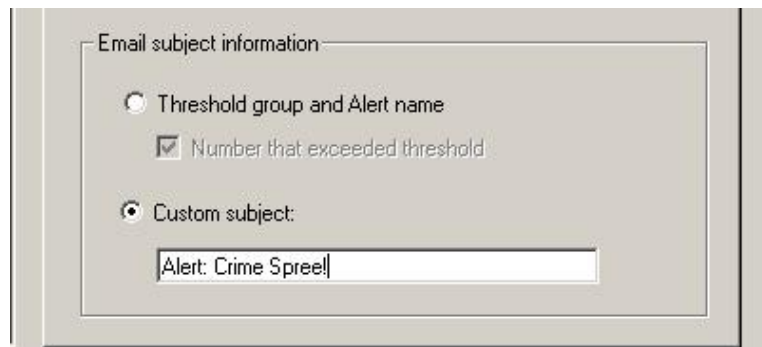


Setting Threshold Alert Emails

After the SMTP servers are set, the email address from which the threshold alerts will be sent must be identified. When personnel receive a threshold alert, this address indicates who sent the alert. Click on the Email Settings tab of the Threshold Alert Setup dialog to enter a valid source email address. A copy of the threshold alert can be mailed to the source address if the option 'Send a copy of this email address...' is selected.



Setting the subject line of the email is also possible from this dialog. Two options exist for the subject line. Either the Group and Name of the alert along with the number that exceeded the threshold can be placed in the subject line of the email, or a standard phrase may be entered.

Attachment A

The screenshot shows a dialog box titled "Email subject information". It contains three radio button options: "Threshold group and Alert name", "Custom subject:", and "Number that exceeded threshold". The "Custom subject:" option is selected. Below it is a text input field containing the text "Alert: Crime Spree!". The "Number that exceeded threshold" option is also checked.

Finally, now that the From email address is set, the email addresses of those personnel that are to receive threshold alerts can be entered. Emails may be sent to any valid email address, however the SMTP Server must be identified for each address.

As mentioned above, the email address entered is automatically assigned a default SMTP server name, if the default is set. If the default SMTP server is not set, a list of available servers is provided from which one must be selected. If a server is not assigned to an email address when the Apply or OK button is hit, a warning message is issued to set the email address' server before continuing.



The screenshot shows a dialog box titled "Email Properties". It contains two main sections: "Recipient information" and "SMTP server information (optional)".

Recipient information:

- Name: Lieutenant Bob
- Email address: Bob@LincolnPD.com
- Do not send email to this address

SMTP server information (optional):

- There is no default SMTP server.
- Select an SMTP server for this e-mail that is different than default
- Email Server Name: [Dropdown menu]

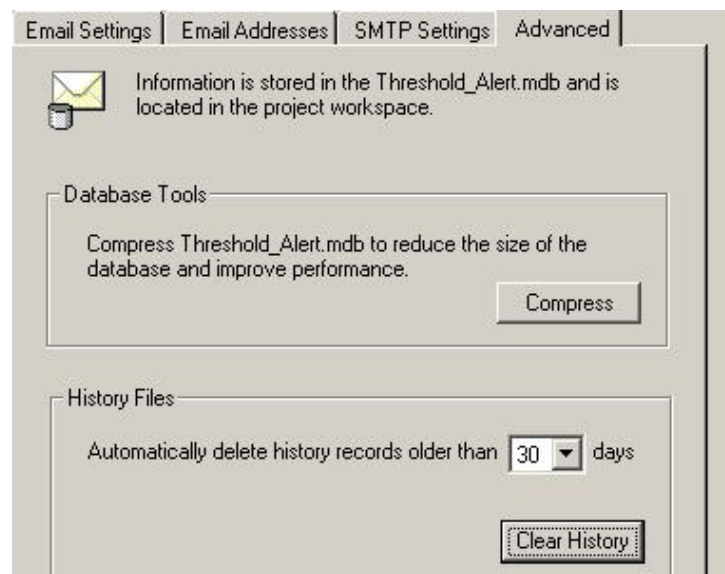
Managing the Theshold Alert Database

Attachment A

Email address and server information is saved to the Threshold Alert database in the project workspace. If many edits to the database are made, it is a good idea to compress the database as it can become large due to the accumulation of edits and deletions.

To compress the database, click on the Advanced tab, and click the button 'Compress'.

The 'Clear History' button is available to keep the size of the database manageable. History records refer to those records that track when a threshold is sent. They should be deleted from the database when this information is no longer required.

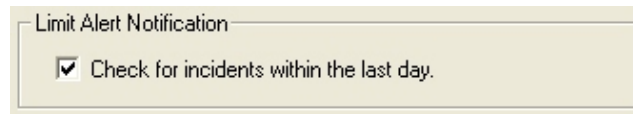
**Limiting Alert Notification**

When a threshold has been reached, a Threshold Alert is sent to the appropriate personnel. The next time the Threshold Alert is run, the same incidents may result in the threshold being reached but the personnel have already been notified. For example, a Threshold Alert has been set to run nightly. The alert checks if there have been 5 incidents within the last 10 days in the downtown district. On Monday night, there are 7 incidents in the downtown district and consequently the Threshold Alert is sent to the local officials. On Tuesday night, there were no new incidents but since there were 7 incidents the day before the threshold has been reached and the Threshold Alert is sent again.

To prevent this repeated notification there is a setting in [OmegaGIS Setup](#) to limit alert notification. On the

Attachment A

Advanced tab, check the "Check for incidents within the last day" checkbox. This setting applies to all Threshold Alerts run. When the Threshold Alert is run manually, there is an option to override this setting.

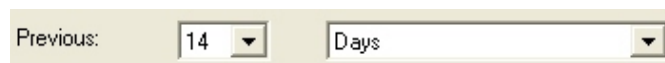


A screenshot of a software interface showing a section titled "Limit Alert Notification". Below the title is a single checkbox that is checked, with the text "Check for incidents within the last day." next to it.

The Limit Alert Notification is used to stop threshold alerts from being sent out repeatedly when there are no new incidents. If 'Limit Alert Notification' is selected in OmegaGIS Setup, Threshold Alert checks the previous day for incidents. If no new incidents have occurred then even if the number of incidents for the date range requested exceeds the threshold value set, the threshold alert is not sent. In this case the threshold alert would simply be a repeat of a threshold alert sent previously. If however, new incidents are found, the date range is searched for previous incidents and a new threshold alert is sent.

Using the 'Limit Alert Notification' requires that data entering the system is kept up to date on a daily basis. Any lag time introduced from the time the incident data enters the system will work against the successful use of Threshold Alert.

The setting only works when the date range specified with the threshold is 'Days', 'Week to Date', 'Month to date' and 'Year to date'. When a different date range is selected, there is no check for incidents within the last day.



A screenshot of a software interface showing a dropdown menu labeled "Previous:". The menu is open, showing a list of options. The first option is "14", which is selected. To the right of the dropdown is a text box containing the word "Days".

When no new incidents are found the email or summary report will state "Threshold Alert was not run as there were no incidents within the last day".

-

Alerts and Notifications

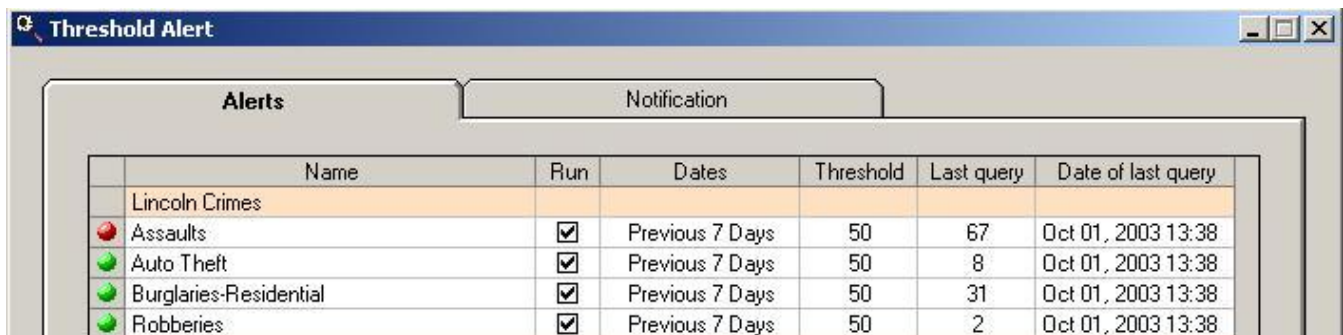
When the Threshold Alert setup is complete, Alerts and Notifications can be organized and run using the Threshold Alert Dialog available from the [Main Menu](#). Alerts refer to the Threshold Alerts that are saved during a Query routine. Notifications are set up to link the Alerts with the email addresses that receive them.





[Alerts Tab](#)

Attachment A[Alert Details](#)[Notification Tab](#)[Running the Alert](#)

Alerts Tab

When a Threshold Alert is first created during a Query routine, it is assigned to a Group, is given a Name, and a specific number of incidents is set as the threshold. The Group can be recognized in the Threshold Alert Dialog by a pink background. Individual Threshold Alerts belonging to this Group are listed below the Group name.



Alerts		Notification				
Name	Run	Dates	Threshold	Last query	Date of last query	
Lincoln Crimes						
 Assaults	<input checked="" type="checkbox"/>	Previous 7 Days	50	67	Oct 01, 2003 13:38	
 Auto Theft	<input checked="" type="checkbox"/>	Previous 7 Days	50	8	Oct 01, 2003 13:38	
 Burglaries-Residential	<input checked="" type="checkbox"/>	Previous 7 Days	50	31	Oct 01, 2003 13:38	
 Robberies	<input checked="" type="checkbox"/>	Previous 7 Days	50	2	Oct 01, 2003 13:38	

In the Threshold Alert dialog, on the Alerts tab, the following columns describe different aspects of the threshold alert:

Name

The name entered when the Threshold Alert was first created during a [Query](#) routine.

Run

Threshold Alerts are run based on the Group to which they belong. To select specific Alerts to run within the Group, the Run checkbox can be toggled to either run or omit the Alert.

Attachment A

Dates

The Date column refers to the duration used to search for incidents that meet the criteria set for the Alert. It is important to note that the duration represents the last complete block of dates. For instance, given that the current date is December 9th, a previous duration of 1 month returns the dates between November 1st and November 30th. The dates between December 1st and the 9th are excluded as they are not a part of a complete month.

Threshold

The Threshold is an arbitrary number that determines when a critical number of events have occurred. When the Threshold is met or exceeded, the pin on the left side of the table for that particular Alert turns from green to red.

Last Query

This column reveals the number of incidents returned by the last query.

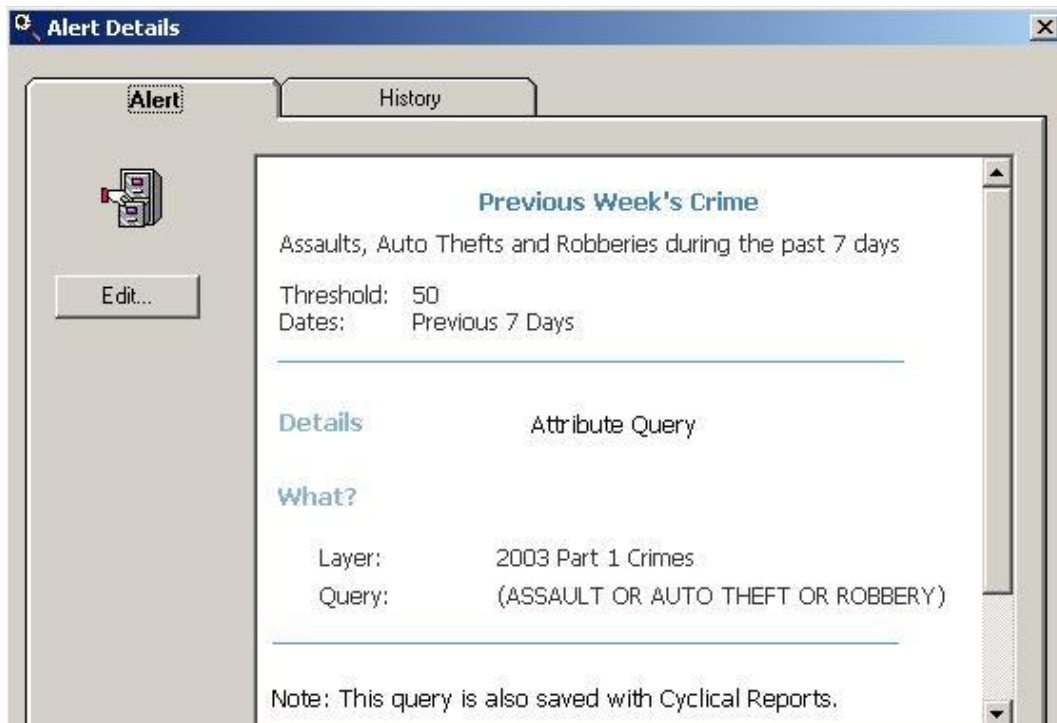
Date of Last Query

As Alerts can be run multiple times, this column displays the last time the Alert was run.

Alert Details

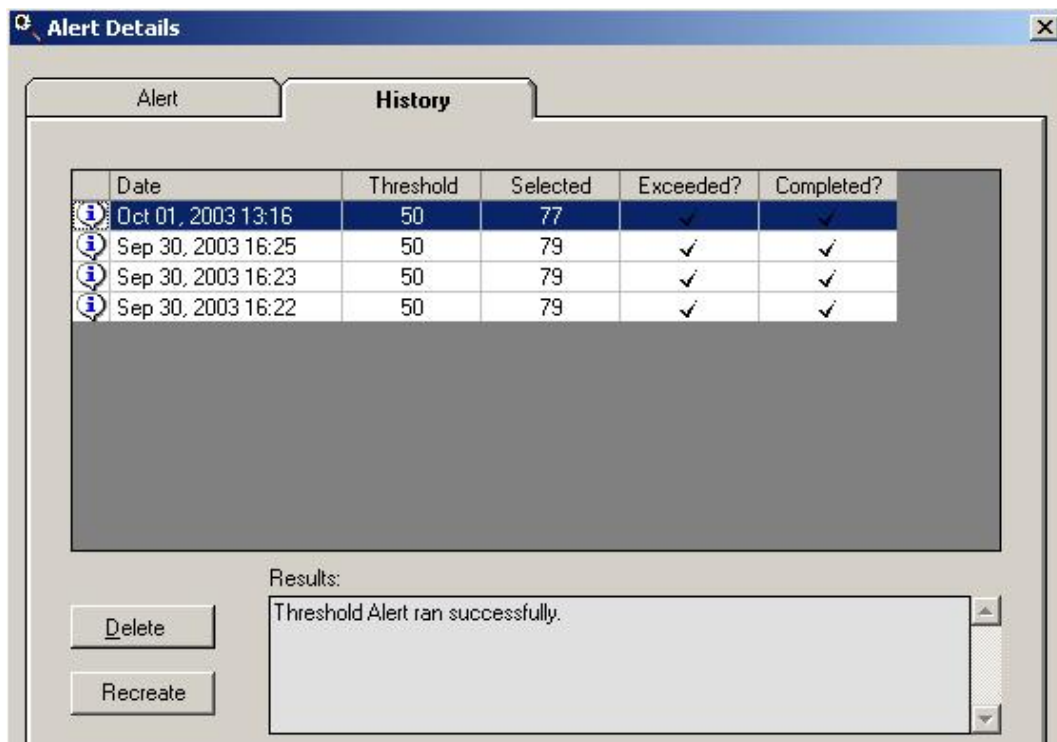
Alert Tab

A detailed description of each Alert within the Group is available by clicking on the Details button. The Alert Details dialog contains two tabs; an Alert tab and an History tab. The Alert tab contains a window summarizing the query used to select the incidents for the Alert. Clicking on the Edit button beside this window, opens the Save Cyclical Report and Threshold Alert dialog where the Group, Name, Description or characteristics of the Threshold Alert may be modified. From this dialog, the Edit button at the bottom of the form returns to the original Query dialog used to create the Threshold Alert initially.

Attachment A**History Tab**

The History tab reveals when the Alert was run previously. The table provided lists the date, the threshold value, whether the threshold was exceeded, and whether the Alert was completed. Clicking on a row in the table, updates the Results window below with a more detailed description about the Alert.

Selecting 'Recreate' runs the Alert using the original date parameters on which the query was based. Before running the Alert, a [Clear All](#) is performed on the project to clear any pre-existing selection sets. Although it would appear that using the original dates should give the same 'snap-shot' of incidents, there may be some differences in the resulting dataset. As the Import Wizard is continually modifying records with the most up to date information from the source database, the number of incidents matching the initial query may have changed.

Attachment A**Notification Tab**

The Notification Tab includes summary information about who is to receive the Threshold Alerts. The Alert is identified by a pink background. Alerts are assigned email addresses which are listed below each Alert. The format and content of the email is set using the options available on the Notifications Group Properties Dialog.

The Alert summary information on the Notification tab includes a listing of the email addresses to which the Alert will be sent. Also found on the dialog is information regarding whether a Group Summary, Map and Report are to be included with the email, as well as whether the email is to be sent only when the threshold is met or every time the Alert is run.

Attach Reports

When the option to include a Crystal Report with the email notification is selected, the Crystal Report is exported to a PDF file. It is this PDF file that is attached to the email. The name of the PDF is a concatenation of the name of the alert item and the report name.

Attachment A

Report Parameters

Typical Crystal Reports are created with parameters that allow for a dynamic report with the user making changes before the report is opened. An example is the title used with the report. When exporting the report to a PDF file, these parameters are suppressed.

Tip: Create a version of the Crystal Report specifically for automation with Threshold Alert.

Email Size

The total size of the email attachment must be taken into consideration. This is especially the case when multiple reports per alert are sent. Typically, an organization will limit the size of email attachments. Emails with attachments larger than the limit are not sent.

Tip: Only include a single report for each alert in an attempt to reduce the size of the email. Another option is not to select the Group Summary. When the Group Summary option is used, all of the alerts are sent in a single email.

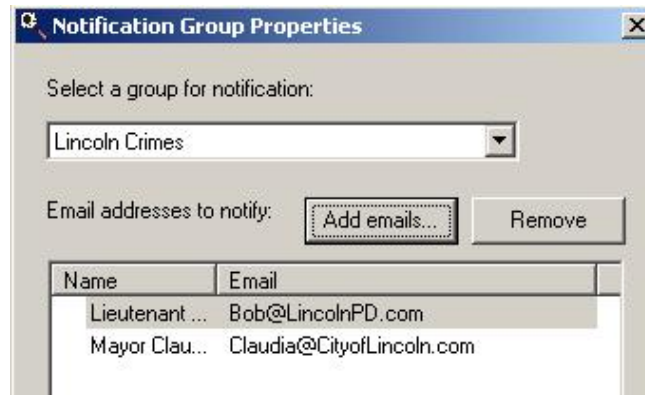
Group Email addresses	Email format	Group summary?	Only when exceed?	Include Map?
Lincoln Incidents Mayor Claudia (Claudia@CityofLincoln.com) Lieutenant Bob (Bob@LincolnPD.com)	Plain text	✓		✓
Lincoln Crimes Officer John (john@LincolnPD.com) Officer Jane (Jane@LincolnPD.com) Mayor Claudia (Claudia@CityofLincoln.com) Lieutenant Bob (Bob@LincolnPD.com)	Plain text	✓	✓	✓

Notification Group Properties Dialog

The Notification Group Properties dialog is accessed from the New or Edit button on the Notification Tab.

Attachment A

This dialog contains options for adding email addresses to a particular Alert as well as setting the format and content of those emails. An Alert Group must first be selected from the list. Clicking the Add emails... button opens a dialog from which the email addresses set up previously using [OmegaGIS Setup](#) can be selected. Each email address selected will receive the Threshold Alert email when it is sent.

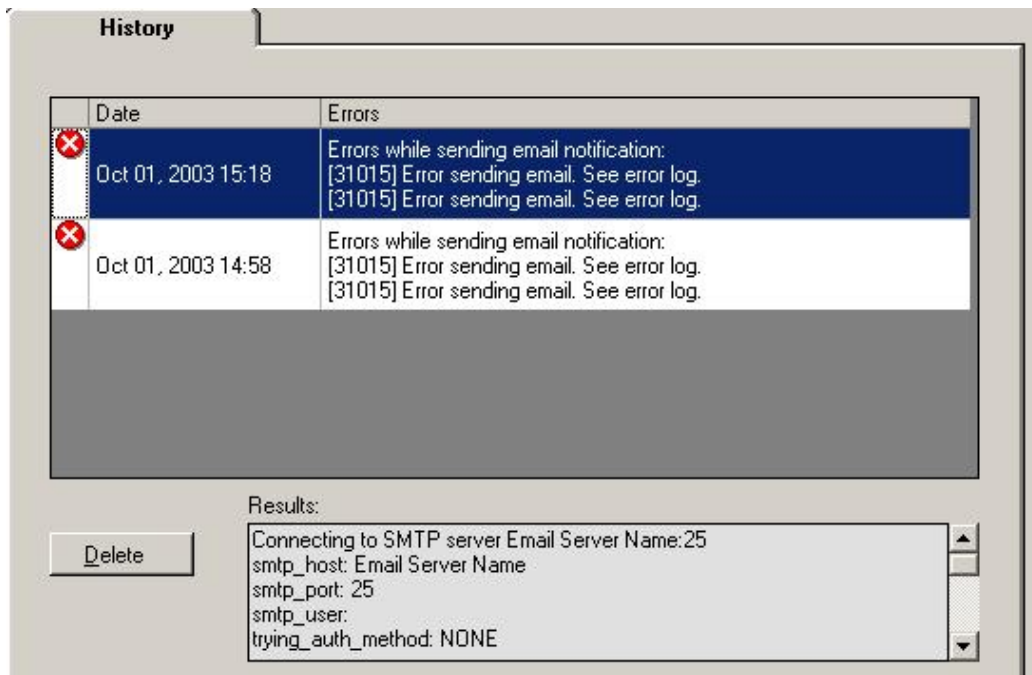


In addition to adding email addresses to a list of recipients, the format and content of the email can also be set. Email can be sent as plain text or in an HTML format, a map can be included in the content of the email or excluded as well as reports, the email can be sent only when the threshold is met, or each time the Alert is run, and the email can contain a Group Summary, or the individual Alert. Each of these items is set for the Alert Group and applies to all of the email addresses within that Group.

It is possible to attach a map image as a .jpg as well as Crystal Reports in PDF format by selecting the appropriate checkboxes on the dialog. If automating the Threshold Alert, the report should not prompt the user for any parameters, such as the report title as this will interrupt the automation of the alert, and it will not be sent.

Notification History

The historical record of a Notification is accessed by selecting a Group on the Notification Tab, and clicking on the History button. The history identifies errors that occur when the Threshold Alert Group is sent by writing an error message to the history list. A list of prior errors is displayed in the table on the form. Clicking on the error, reveals more information in the Results window below.

Attachment A

Running the Alert

Although Alerts can be set to run automatically, they can also be run directly from the Threshold Alert dialog by clicking Run. A small dialog opens, and an Alert Group can be selected from a drop-down list.

There are a few options that can be activated once Threshold Alerts are completed:

Show Summary

With this setting selected, the Threshold Alerts summary dialog opens when processing is complete. This dialog contains information on each of the Threshold Alerts that were run.

Email Results

With this setting selected, email notifications are sent to the appropriate personnel.

Check for Incidents Within the Last Day

Attachment A

With this setting selected, it is determined whether there have been any incidents within the last day before proceeding to run the Threshold Alert. The checkbox is selected based on the setting in [OmegaGIS Setup](#).

Either the Show Summary or the Email Results checkbox must be selected for the Run button to be enabled. Running the Alerts manually provides an easy method to check whether Notifications are sent properly before the system is automated.

Automating Threshold Alerts

When Threshold Alerts and their corresponding Notifications are set, it is possible to automate the process of alerting personnel when incidents exceed a certain threshold. Automating the distribution of information allows personnel to be notified of significant events, while removing the need to search through repetitive analysis queries for spikes in the number of incidents.

It is extremely important that if automating reports, parameters such as prompting the user for a title not be included. Using parameters interrupts the automation of the threshold alert so that it cannot be sent.

The Microsoft Windows Task Scheduler

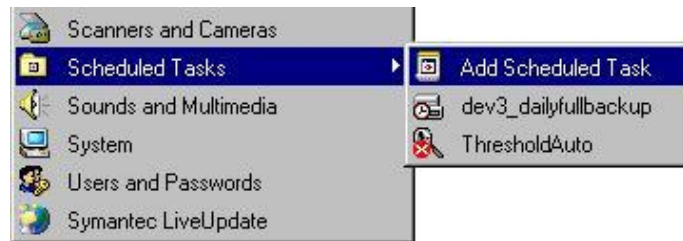
The Microsoft Windows Task Scheduler handles the automation of Threshold Alert. The Task Scheduler is already installed on Microsoft Windows 2000 and XP operating systems.

To create a new task using Microsoft Windows Task Scheduler:

From the Windows Start button...

Attachment A

- Select Settings/Control Panel and then Scheduled Tasks.
- Select Add Scheduled Task



In the Task Scheduler wizard...

- Select the ThresholdAuto.exe as the program to be run by Windows
- Use the Browse button to locate the ThresholdAuto_2.exe

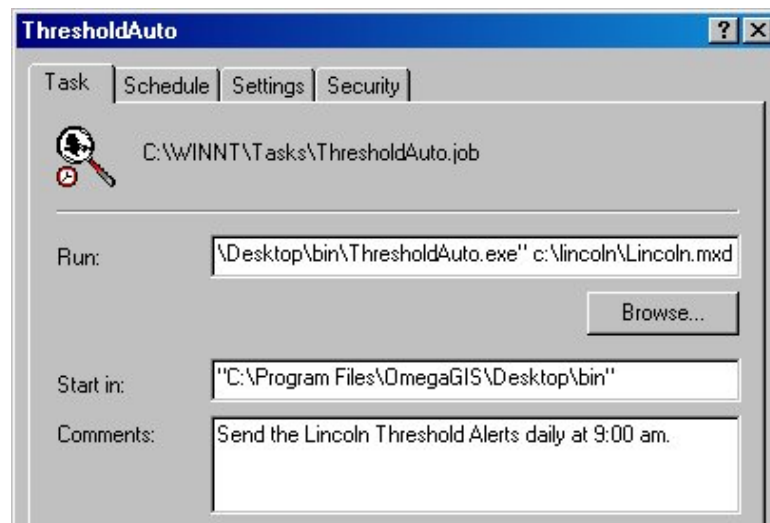
(Installed on the C:\Program Files\OmegaGroup\Desktop\Bin)

Note: ThresholdAuto_2.EXE was introduced at the Omega Desktop 4.3 release and it is an upgrade to the ThresholdAuto.EXE. The ThresholdAuto.EXE will continue to work but it is recommended that new implements use the ThresholdAuto_2.EXE.

- Enter a name for the task and select when to perform the task.
- Enter the Windows user name and password. The task will run under the permissions of this user.

Attachment A

Note: Using the password of the current user requires that the user be logged in for the automated task to complete successfully.



When task wizard is completed open the advanced dialog...

Add the path to the ArcMap document to the command line.

On the Task tab on the Advanced dialog, add the ArcMap document path at the end of the existing command line. The path to the ThresholdAuto.exe should be in double quotes due to spaces in the file names. For example: "C:\Program Files\OmegaGroup\Desktop\Bin\ThresholdAuto_2.exe" c:\CrimeView\MyMaps.mxd

If there is an error automating the Threshold Alert, the [Write File.EXE](#) utility may provide trouble shooting information.

Note: This ArcMap document should already contain Threshold Alerts with email notification. See the help document for how to create Threshold Alerts.

When ThresholdAuto.exe is run, a log file, ThresholdAlert.log, will be written to the ArcMap document's [project workspace](#). For the document c:\CrimeView\MyMaps.mxd, the log file would be found at c:\CrimeView\MyMaps\ThresholdAlert.log.

Omega Data Manager

The preparation of accurate source information on which to base geographic analyses is important to the GIS process. The Omega Data Manager contains tools available as an extension to ArcCatalog to assist in preparing standardized, accurate data for use with Omega Desktop routines.

The extension includes the following tools:

[Saved Queries Editor](#)
[Metadata Editor](#)
[OmegaGIS Field Manager](#)
[Demographic Data Loader](#)
[Clone Omega Metadata](#)

Accessing the Extension

Before any of the tools can be used, the Omega Data Manager extension must be enabled. To enable the extension follow the these steps:

- Open ArcCatalog and from the Tools pull-down menu select Extensions.
- Select the checkbox next to "OmegaGIS Data Manager". The extension is protected from unauthorized use; at least one Omega Desktop product, such as CrimeView or the Omega Import Wizard, must be licensed for extension to be enabled.


After the Omega Data Manager extension is enabled, the toolbar must be added to ArcCatalog. This is done by selecting Toolbars from the View pull-down menu in ArcCatalog. From the list of toolbars select 'OmegaGIS Data Manager'.

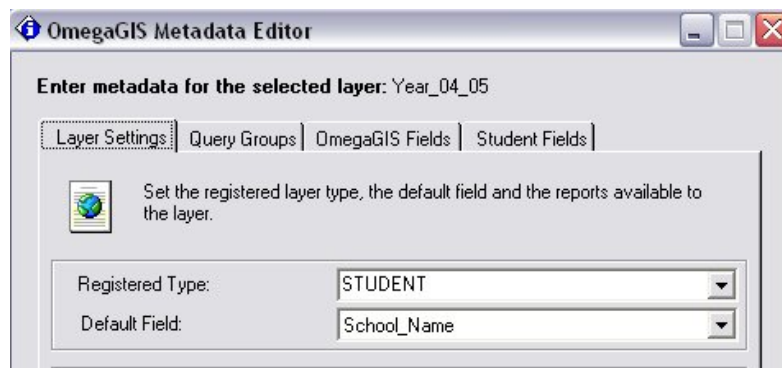
OmegaGIS Metadata Editor

Metadata is descriptive information about data. OmegaGIS uses metadata to increase performance as well as store commonly used parameters that are necessary for OmegaGIS routines. The OmegaGIS Metadata Editor is available as one of the OmegaGIS Data Manager tools in ArcCatalog. It provides a dialog to set information common to most OmegaGIS routines.

[Accessing the OmegaGIS Metadata Editor](#)
[Feature Class Geometry Types](#)
[OmegaGIS Metadata Editor Dialog](#)
[SchoolPlanner™ Metadata](#)

Accessing the OmegaGIS Metadata Editor

To view metadata for a dataset, select the desired object in ArcCatalog and use the Metadata Editor button  on the Omega Data Manager extension toolbar to open the editor. This button is only available when the Omega Data manager extension is enabled and the selected object is a feature class with the geometry type of point, multi-point, polygon or line. The feature class may be stored in a File Geodatabase, Personal Geodatabase, ArcSDE or shapefile format.



When the feature class is stored in ArcSDE, the spatial database connection used to connect to the feature class must be the owner of the feature class. That is, the same login that generated the feature class must be used to update the metadata of that feature class.

Attachment A**Feature Class Geometry Types**

There are four main geometry types that are supported in the Metadata Editor. These types include, point, multipoint, polyline and polygon. It is important to distinguish between these types, as certain options on the Metadata Editor are available to some types and not others. If an option is unavailable to a particular feature type, the option is disabled and may not appear as an option, or a warning message may be displayed.

Point Geometry Type

A point layer can access all of the options on the Metadata Editor Dialog, with the exception of options that are reserved for specific registered types.

Polygon and Polyline Geometry Type

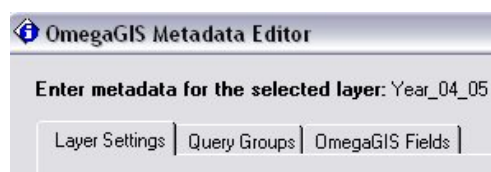
Options available to polygon or polyline layers are limited to Registered Type, Default Field, and an associated Density Map Report. A polygon layer might represent a city boundary, an example of a polyline layer might include streets or rivers. The other options are not displayed on the dialog by default. If a specific registered type is selected, then other options related to that type may appear such as the Facility Name Field option associated with the School Boundary registered type.

**Multipoint Type**

Using OmegaGIS, a multipoint type layer is generated by the Repeat Calls routine. The layer identifies the source of multiple crimes. The Metadata Editor options available to this type of layer include the registered type, the default field and the repeat calls report option.

OmegaGIS Metadata Editor Dialog

The Metadata Editor has a number of settings that attach metadata information to the data selected in ArcCatalog. Layer Settings, Query Groups and OmegaGIS fields are represented by three tabs available at the top of the dialog. By clicking on each of these tabs, metadata for each of these categories can be set. The Query Groups and OmegaGIS Fields tabs are not available to polygon, polyline or multipoint layers. In addition, if the Student registered type is selected, then additional tabs specifically related to student metadata used by SchoolPlanner™ will appear. For more information on the SchoolPlanner™ metadata, [see the SchoolPlanner™ section in this document.](#)

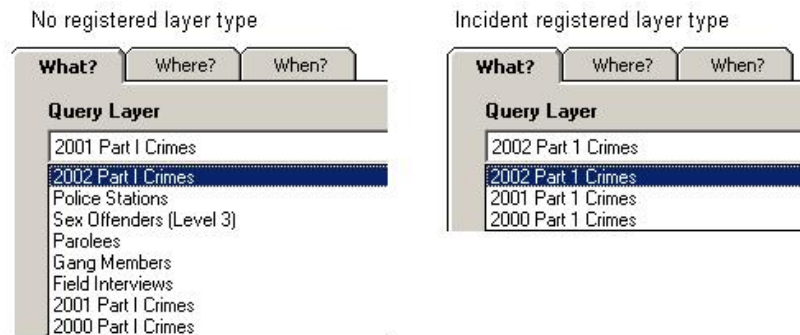
**Layer Settings**

Registered Type

Attachment A

A layer's registered type assigns the layer to a user specified category. The default registered types available for point layers include Incident, Student, Station, Person and Other, while polygon layers may be assigned to the Census_Blockgroup, Census_Block, Census_Tract, or Other layer types. In the event that additional types are required, the user may type them into the text box that provides the predefined list.

The benefit to assigning registered types arises when a project becomes complex with many different layers. Without the registered type, all layers are available to OmegaGIS routines regardless of whether or not they are compatible with the type of analysis to be performed. By adding a registered type to layers in a project, the layer list is limited to only those layers appropriate to the selected routine. Options are available in [OmegaGIS Setup](#) to determine whether to use the registered type to limit the layer list, as well as to select which registered layer type(s) to use.



It is important to note that if the option in OmegaGIS Setup is selected to limit the layer lists on OmegaGIS dialogs, only layers of registered types will be shown. All other layers are omitted from the lists.

Default Field

The default field is automatically selected by OmegaGIS routines if it is set in the Metadata Editor. It applies to boundary layers, where the 'By Field Value' option is used to select polygons in the layer based on a particular field in the attribute table. Setting the default field in advance bypasses the need to select the field of interest each time a new routine is run. Setting the default field becomes especially efficient when there are a large number of fields within the layer to sort through.

**Default Incident Graph Field**

The default incident graph field is used as the default field when creating graphs for an incident layer. The default field is set automatically if it can be found. If not found, each time a graph is created, a field must be selected in order to identify the data that should be graphed.

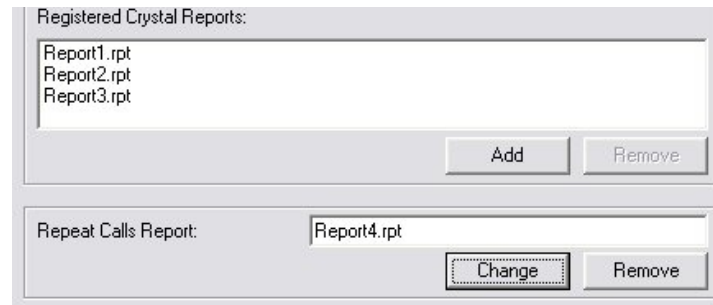
Registered Crystal Reports

The reports referred to in the Metadata Editor are designed in Crystal Reports to display information contained in the data layers. These reports can be viewed through the ['Create Reports'](#) tool available on the OmegaGIS Toolbar in ArcMap. However, they must already be registered to the appropriate layer.



Attachment A

When registering reports using the Metadata Editor, one or more report may be selected for a single layer. The 'Add' button on the Layer Settings tab can be used to browse for reports that have been created for the layer of interest. Notice that in the figure below, the path to the report is not saved. The default location for reports is within the [project workspace](#) \reports folder. For instance, in the project C:\MyProject, the default report folder is C:\MyProject\Reports.



If additional report locations are required, [OmegaGIS Setup](#) can be used to create these search locations. For instance, the 'Create Report' tool must find the report selected in order to display it. Since the report path is not saved with the report name, the first location searched is the default report location within the project workspace \reports folder. If the report is not located, each subsequent path in the OmegaGIS Setup Crystal Report list is searched.

Repeat Calls Report

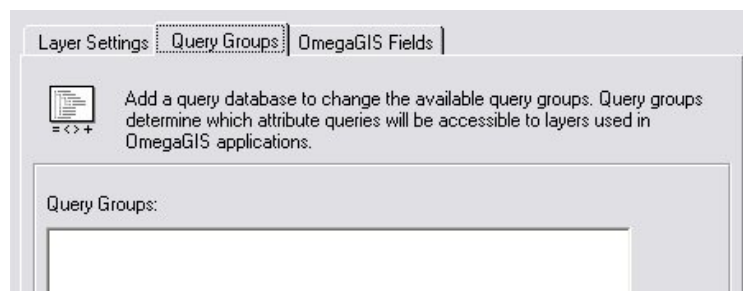
The Repeat Calls Report is used exclusively for layers that have the 'Repeat Calls' report registered to them. A layer may be registered with this report either through the OmegaGIS Metadata Editor, or automatically when it is created with the OmegaGIS [Repeat Calls routine](#). The result of the routine is a multipoint layer that identifies the locations of multiple incidents. The new layer contains the 'Repeat Calls Report' metadata as it is copied over from the layer on which the analysis was based.

Density Map Report

A Density Map Report can be registered to any polygon layer using the Density Map Report setting. This setting replaces the 'Repeat Calls Report' setting when the Metadata Editor is opened while a polygon feature class is selected. Registering a Density Map Report to a polygon layer, ensures that the report can be opened through the ['Create Reports'](#) tool when the appropriate polygon layer is selected.

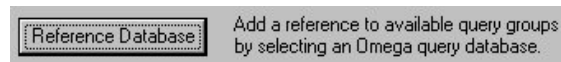
Query Groups

A query group is a container housing related queries that are commonly used with OmegaGIS routines. Query groups are designed during the initial stages of a project, and can be created using the 'Saved Queries' tool found in the OmegaGIS Data Manager extension in ArcCatalog. All of the OmegaGIS routines use the Saved Queries tree to display query groups. When a layer is selected for use in an OmegaGIS routine, the query groups registered to the layer are displayed.

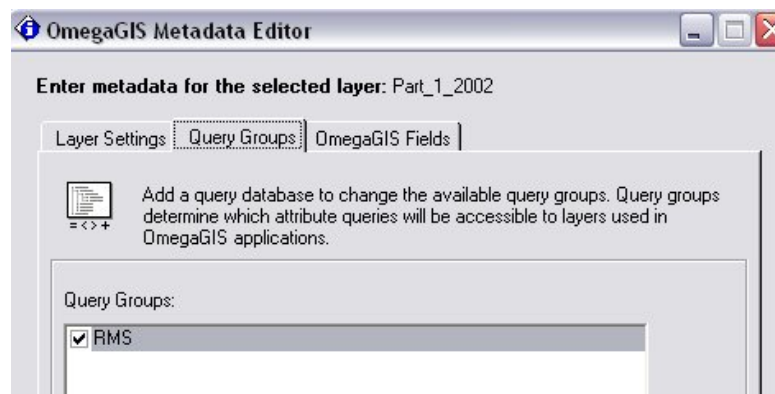


Attachment A

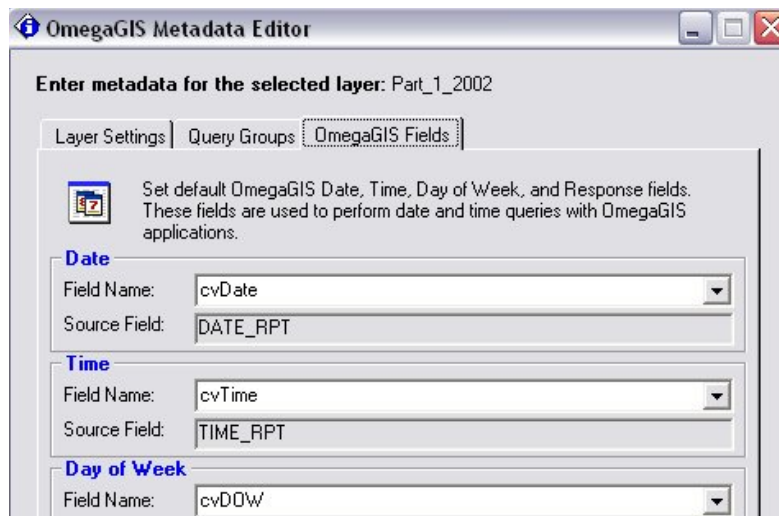
To access and link the query groups to a layer, a reference must be made to the Saved Query Database. The database is commonly located in the project folder. For instance, the database for C:\MyProject is found in the same folder; C:\MyProject. The reference is created by clicking on the 'Reference Database' button within the Query Groups tab of the OmegaGIS Metadata Editor.



Once a database is selected, the query groups found within the database are listed in the Query Groups window. Clicking on these query groups registers them to the selected layer, and makes them available in the Saved Queries Tree during an OmegaGIS routine.

**OmegaGIS Fields**

OmegaGIS fields are used to query data based on date ranges or response times. OmegaGIS fields can only be created using Import Wizard or the [Omega Field Manager](#). Legacy fields such as cvDate and cvTime created in the 3.x product can be used with Omega routines, however they will not show up as options in the OmegaGIS Default Field lists in the MetaData Editor. Multiple date and time fields are supported; the Metadata Editor allows the user to select a default date, time, response time, and response time 2 field that will be used with OmegaGIS routines.



SchoolPlanner™ Metadata

The SchoolPlanner™ registered types include Student, Housing, and School field options for point layers, and School Boundary and Census types for polygon layers. Census registered types have been further refined to selections of Census_Block, Census_Blockgroup, and Census_Tract in order for Omega routines to differentiate between the layers use.

SchoolPlanner™ Layer Settings

School Boundary (Polygon)

If the School Boundary registered type is selected then an additional field to enter the Facility Name Field will appear. This field is used throughout OmegaGIS routines primarily for reporting considerations.

Census_Block, Census_Blockgroup, Census_Tract (Polygon)

Census layers do not require the registration of additional metadata information outside of the default polygon information, which includes the default field and an optional density map report.

Student (Point)

When a student layer is registered, aside from requiring the default point layer information, a Student Fields tab will also activate. Since the student layer is used in many SchoolPlanner™ routines, both analysis and reporting, additional metadata information is required. Fields that must be entered are marked by being contained within the Required section. These fields include:

<i>Numeric Grade</i>	Field containing the grade of the student.
<i>Attending School Name</i>	Field containing the name of the students school of attendance.
<i>Descriptive Grade</i>	Field containing the description of the grade of the student (ie: Kindergarten for 0).
<i>Student Year</i>	The applicable academic year of the student data (ie: 2004-05). The entry must be in the hyphenated format "yyyy-yy" in order to validate, where yyyy is the full first year and yy are the last two digits of the second year.
<i>Minimum Grade</i>	The minimum grade of the students used in the field. The minimum value for all of the

Attachment A

students will be automatically calculated when the Numeric Grade Field is entered. The value can be adjusted for reporting and analysis purposes in order to use a subset of the available grades if necessary.

Maximum Grade

The maximum grade of the students used in the field. The maximum value for all of the students will be automatically calculated when the Numeric Grade Field is entered. The value can be adjusted for reporting and analysis purposes in order to use a subset of the available grades if necessary.

The optional fields and reports should be set if available or as needed since the presence of their values will simplify the operation of Omega routines. Optional fields include:

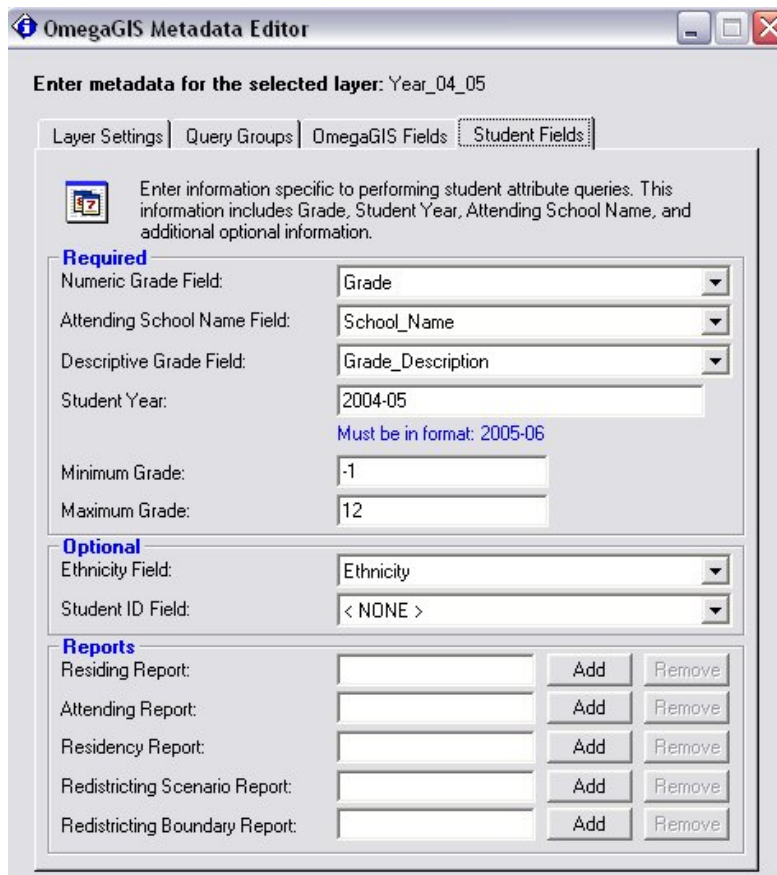
Ethnicity

Field containing the ethnicity of the student. Used primarily for reporting.

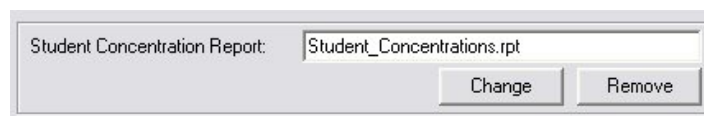
Student ID

Field containing the Student ID number of the student. Used primarily for reporting.

Crystal reports (rpt extension) can be associated with the student layer to allow for rapid reporting of different common tasks. Add a report by browsing to its location by pressing the Add button next to the report and selecting it from the file browser. When the file has been added, it will appear in the box beside the report. To remove the report simply press the remove button associated with the report. The reports that can be associated with a layer include the Residing Report, Attending Report, Residency Report, Redistricting Scenario Report, and the Redistricting Boundary Report.



Additionally for student layers, the option to register a Student Concentration Report will appear under the Layer Settings tab.



Housing (Point)

Attachment A

Registering a layer as housing will activate an additional Housing Fields tab. This tab will allow the entry of metadata that will record additional fields used by OmegaGIS analysis and reporting routines. These include the Student Generation Rate field, the Development Name Field, and fields to indicate up to five years of data to base housing based trend analysis on. There is also a field that will allow the name of the developer to be recorded.

School (*Point*)

No additional information is required outside the default information for a regular point layer if a layer is registered as a School layer.

OmegaGIS Stylesheet

Stylesheets are documents that enable the display of metadata in different styles. They are similar to queries in that they work on the same information, but the output of the data can be viewed in alternate formats. There are a number of stylesheets provided with ArcCatalog. To view the stylesheets, select a dataset in ArcCatalog, click on the Metadata tab, then click on the Stylesheet listbox available on the ArcCatalog toolbar.



OmegaGIS Stylesheet Overview

- [The Project XML](#)
- [OmegaGIS Stylesheet](#)
- [Update Information](#)
- [Dataset Date Range](#)
- [Report Information](#)
- [Import Profile](#)
- [OmegaGIS Fields](#)
- [Geocoding Information](#)
- [Output Information](#)
- [SQL Query Information](#)

Attachment A**The Project XML**

The OmegaGIS stylesheet is provided as a part of OmegaGIS. The stylesheet reads information in the project's XML document and displays it in a standard format. The project's XML document is located in the project folder and carries the same name as the project. For example, if the project is called MyProject.mxd, and is located in the c:\MyProject folder, the XML document is c:\MyProject\MyProject.xml.

Each time an OmegaGIS routine is run, the project XML document is updated with specific information recorded by the routine. This information is used to reset the dialog selections when the dialog is opened the next time. In this way, updating all of the settings on the dialog each time a routine is run is avoided. The following figure provides an example of the information that is recorded in the project XML document during an Exception Reporting routine.

```

- <omegagis>
- <exceptionreporting>
- <what>
  <previouslayer>2002 Part 1 Crimes</previouslayer>
  <currentlayer>2003 Part 1 Crimes</currentlayer>
  <newlayer>2003-2002 Comparison</newlayer>
+ <queries>
</what>
<date>2003/10/13</date>
<time>12:45</time>
- <where>
  <transparency>20</transparency>
  <belowline>0</belowline>
  <boundarylayer>Police Beats</boundarylayer>
  <boundaryfieldname>BEATS</boundaryfieldname>
  <selectionmode>By Field Value</selectionmode>
- <fieldvalues>
  <value>1A</value>
  <value>1B</value>
  <value>2A</value>
  <value>2B</value>
</fieldvalues>
</where>
+ <when>
</exceptionreporting>

```

The project XML document can be viewed in Internet Explorer by double-clicking on the document name in Windows Explorer. Editing the document in any way is not a good idea, as an invalid format cannot be read by the OmegaGIS stylesheet. If the XML document does not exist, or is damaged in any way, it can be deleted as it is recreated automatically by the OmegaGIS routines.

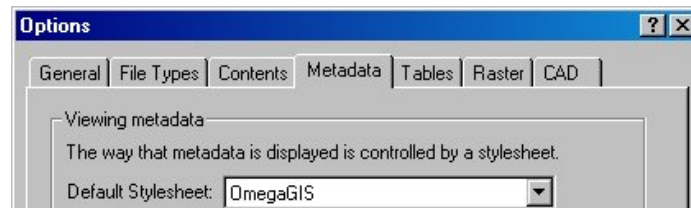
OmegaGIS Stylesheet**File Location**

Stylesheets used in ArcGIS must all be located in the ArcGIS stylesheet folder. This folder is found in c:\arcgis\arcexe82\metadata\stylesheets where arcexe82 represents the version of ArcGIS. In upgrading ArcGIS from 8.2 to 8.3, it becomes apparent that the location of the stylesheets is changed slightly. Instead of being located under the \arcexe82 branch of ArcGIS, it is now located under \arcexe83.

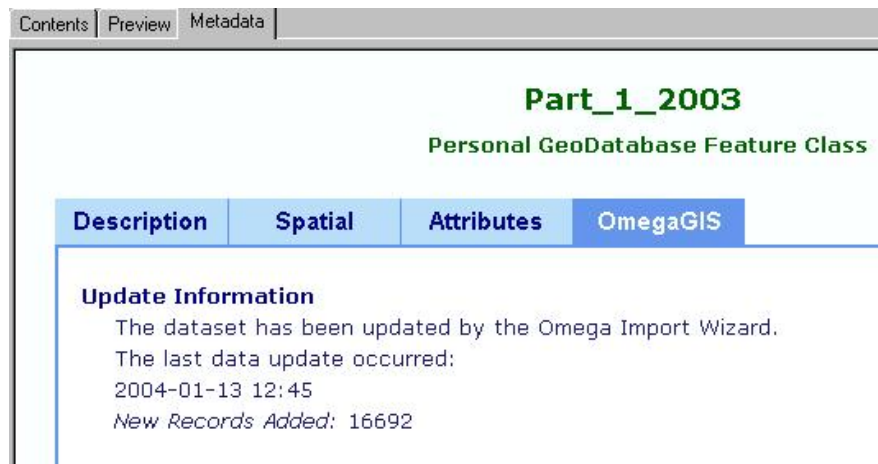
For this reason, OmegaGIS automatically loads the OmegaGIS stylesheet into the appropriate folder based on the current version of ArcGIS. This process takes place both when OmegaGIS is installed as well as when the OmegaGIS Metadata Editor is opened. If for some reason, the OmegaGIS.xml file is missing from the \arcexe* folder, and is not copied automatically, it can be manually copied from the OmegaGIS installation folder; c:\program files\omegagis\common\style

Setting a Default Stylesheet

To set the OmegaGIS stylesheet as the default, click on the Tools menu, select 'Options', and choose the Metadata tab. Select 'OmegaGIS' from the drop-down list as the default stylesheet.

Attachment A**Viewing the OmegaGIS Stylesheet**

To access the OmegaGIS stylesheet, click on OmegaGIS in the stylesheet list if it has not already been set as the default. The format of the OmegaGIS stylesheet follows that of the FGDC ESRI stylesheet. The only difference is the addition of the OmegaGIS tab which displays OmegaGIS specific information. The following sections provide a brief description of the metadata that the OmegaGIS stylesheet provides.

**Update Information**

In setting up a project, an import process can be created to retrieve records automatically from a source database. The Omega Import Wizard is used to generate this process. Update Information provides the date and time of the last data import, as well as the number of new records added.

Dataset Date Range

While using the Import Wizard to process data, an option can be set to search the layer for the range of dates that have been imported. The date range can then be used by the Omega Date-Time dialog to automatically update the calendars with the available dates. The format of the date is yyyyMMdd.

Dataset Date Range

The field used to calculate the date range was: cvDate
 The following date range is available.
Begin Date: 20020101
End Date: 20021231

Report Information

Report information summarizes layer metadata that has been set using the OmegaGIS Metadata Editor <LINK>. Descriptions of Registered Reports, Query Groups, Registered Type, and the Label Field are all outlined in the OmegaGIS Metadata Editor document.

Import Profile

The information in the Import Profile section of the stylesheet is compiled by the Import Wizard. When an import profile is created, the following information is updated:

ID

Attachment A

The ID is generated automatically by the Omega Import Wizard. It uniquely identifies an Import Profile.

Name

The Name refers to the name of the Import Profile, entered when the Profile is first created with the Omega Import Wizard.

Type

There are two types of connections that can be made when creating an Import Profile. The type is identified either as a 'Database Connection' or a 'Text Import'.

Version

The version information is a reflection of the Revision History available in the Profile Overview of the Import Wizard. The version number is automatically updated as changes are made to the Import Profile.

OmegaGIS Fields

OmegaGIS Fields are used by the Date-Time dialog in OmegaGIS routines to determine date and time ranges. OmegaGIS Fields are created using the OmegaGIS [Field Manager](#) in the Omega Data Manager extension in ArcCatalog. The name, type, source field and whether the field is selected as the default are listed in a table in the stylesheet.

Geocoding Information**Geocoding Service**

In this section of the stylesheet, Geocoding Services and Geocoding Statistics are defined for the layer. Geocoding Services refer to the process used to convert non-spatial information into spatially referenced data that can be used in spatial analysis.

The first column in the table identifies the name of the Geocoding Service. A Geocoding Service is created in ArcCatalog where a name is assigned to the service. The second column of the table shows the geocoding service style used to create the geocoding service. There are numerous geocoding service styles including 'Single Field' and 'US Streets'.

Geocoding Service	Style
Lincoln Streets	US Streets

Intersection Connectors: / &

Within the address field of a dataset, various text characters are used to represent street intersections. When designing a Geocoding Service, Intersection Connectors, are those textual delimiters that create the intersection in the address. More than one connector can be incorporated into a Geocoding Service.

Geocoding Statistics

When a layer is geocoded against a source dataset, it is rarely the case that all records are matched up to a source location. In many cases, the address may not be found, in which case the record is not given a feature on the map. Understanding Geocoding Statistics is important when trying to identify why features are missing from the new layer, even though they have been imported by the Import Wizard process.

A quick overview of geocoding statistics is possible with the OmegaGIS stylesheet. The following statistics are valid for the last time the import process was run.

Overall Match Rate

The overall rate is the number of records matched divided by the total number of records processed.

Matched

This statistic refers to the number of records matched to an address.

Unmatched

Unmatched refers to the number of records that could not be matched to an address or a coordinate.

XY Coordinate Match

The XY Coordinate Match is the number of records matched to an XY coordinate.

Total Features

This statistic refers to the total number of features processed.

Output Information

Attachment A

As data is retrieved from the source database or text file using the Omega Import Wizard, it is processed, and output into a new file. There are several methods of moving the data to the new dataset. Each of these Output Types can be identified with a number between 0 and 6. The number indicates the way in which new features are appended to the dataset.

It is extremely important to recognize the difference between Output Types, as the type used to process the records can produce very different results. The Output Types available in the Omega Import Wizard are outlined below.

New Feature Class [0]:

Creates a new feature class. Will not overwrite an existing feature class.

Replace Feature Class [1]:

Deletes the existing feature class, if any, and then creates a new feature class.

Append Only [2]:

Appends records to an existing feature class; no duplicate records are removed. If the existing feature class is not found then a new one is created.

Remove Duplicate Records [3]:

Removes duplicate records in the feature class that is being appended to based on a primary key. Once the duplicate records are removed, the new records are appended. If the existing feature class is not found then a new one is created.

Remove Duplicate Records with Date Range [4]:

Removes duplicate records in the feature class that is being appended to based on a primary key. Once the duplicate records are removed, the new records are appended. If the existing feature class is not found then a new one is created. After the appending process, the feature class is queried to remove old records based on a date range.

Append Only with Date Range [5]:

Appends records to an existing feature class; no duplicate records are removed. If the existing feature class is not found then a new one is created. After the appending process, the feature class is queried to remove old records based on a date range.

Truncate Feature Class [6]:

Deletes all records from an existing feature class, if any, and then inserts the new records. This output type should be used with a feature class stored in ArcSDE rather than the Replace Feature Class output type.

SQL Query Information

If a database connection is used to extract records from the source database, the SQL statement can be viewed from the OmegaGIS stylesheet. The SQL statement is valuable if field names or tables change in the source database. The statement can be reviewed and compared to the source database to catch any revisions made to the source.

```
SELECT: Incident.Address, Incident.Call_Type,
Incident.Comments, Incident.Case_Numbe, Incident.Status,
Incident.Day_From, Incident.Time_From, Incident.Day_To,
Incident.Time_To, Incident.Date_From, Incident.Date_To,
Incident.Officer, Incident.Loss, Incident.Damg,
Incident.Loc_Code, Incident.Type_Code, Incident_Date_RPT,
Incident.Time_RPT
FROM: Incident
WHERE: Incident.Date_RPT Between ('2003-01-01') AND
('2003-12-31')
```

OmegaGIS Fields Manager

The OmegaGIS Fields Manager creates OmegaGIS fields used with the [date and time](#) Query dialog. The OmegaGIS Fields Manager can convert a user specified source field to a new field with the format required by OmegaGIS routines.

In most cases Omega Import Wizard is used to create OmegaGIS fields; this tool has been developed to aid in creating these same fields in a non-automated fashion.

[OmegaGIS Fields](#)

Attachment A

[Adding, Removing and Updating OmegaGIS Fields](#)

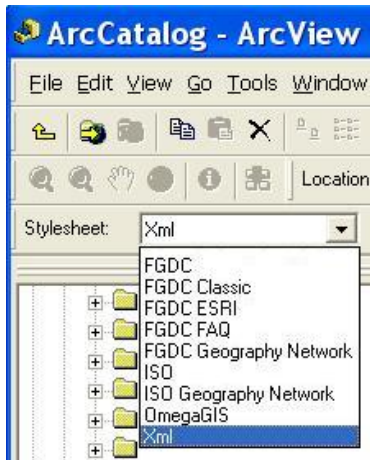
[Adding an OmegaGIS Field](#)

[Removing an OmegaGIS Field](#)

[Updating an OmegaGIS Field](#)

OmegaGIS Fields

The OmegaGIS Fields Manager provides a means to add, edit and delete OmegaGIS Fields. An OmegaGIS Field is defined by metadata found in the XML that is associated with the dataset. To view a dataset's metadata, select the data in question in the ArcCatalog table of contents. When the data is selected, use the drop-down stylesheet list box and select the XML option.



A stylesheet is a tool for viewing XML tags. There are many variations of stylesheets available that display the XML tags in different formats. The XML stylesheet displays the XML metadata tags without modification. Once the XML stylesheet is selected, the right side of the window displays the metadata tags. OmegaGIS fields can be identified as those tags that occur within the 'theomegagroup\importwizard\omegagisfields' XML node.

For each OmegaGIS field, a name, type, source, format, description and a tag that indicates whether the field is set as the default are stored. It is very important that the information within this XML document only be modified using the OmegaGIS Field Manager or the OmegaGIS Metadata Editor. Attempting to modify the information without these tools may corrupt the data.

```
<theomegagroup>
- <importwizard>
+ <profile_info>
+ <update>
+ <append>
+ <sqlimport>
- <omegagisfields>
- <field>
  <name>Alarm_Date</name>
  <type>Date</type>
  <source>alarmdate</source>
  <description>REQUIRED</description>
  <format>11</format>
  <source1 />
  <format1 />
  <default>1</default>
</field>
```

Note: In the ArcView 3.x version of Omega products an OmegaGIS field was identified by name as 'cvDate', 'cvTime' or 'cvDOW'. The limitation on this form of identification was that only one field could be used by OmegaGIS routines to identify date and time ranges. The fields created in the 3.x product cannot be used in the new product as OmegaGIS fields. Use the 'Add a new OmegaGIS Field' option in the OmegaGIS Fields Manager to recreate these fields.

Attachment A**Adding, Removing and Updating OmegaGIS Fields**

The OmegaGIS Field Manager provides a means for adding, editing or removing an existing OmegaGIS field. The utility is provided on the OmegaGIS Data Manager extension in ArcCatalog. This tool is only available to those datasets with point feature geometry. While clicking on different datasets, the Fields Manager tool is either enabled or disabled depending on the feature geometry of the dataset selected.



When the OmegaGIS Fields Manager dialog is opened, three options are presented to the user; Add, Remove or Update an OmegaGIS field.

**Adding an OmegaGIS Field****Field Type**

If the 'Add a new OmegaGIS Field' option is selected, clicking on the 'Next' button opens a dialog that presents a list of OmegaGIS field types that can be created. The list includes 'Date', 'Time', 'Response Time' and 'Response Time 2' fields. The first step in defining a new OmegaGIS field is to select the field type to create. The field types available are described below.

Date

Selecting the 'Date' type creates a new OmegaGIS field formatted as an eight character numeric field. The format is as follows: yyyyMMdd. Once created, the new date field can be used to select dates from the calendars on the Date/Time dialog which is common to many routines.

Time

The 'Time' field type creates a string field of four characters formatted as 'hhmm'. The new OmegaGIS time field can be used to select from the drop-down lists on the Date/Time dialog which is common to many routines.

Response Time

The 'Response Time' field type generates a new OmegaGIS response time field using a start time field and an end time

Attachment A

field found in the data. The response time is created as a number with two decimal places. During the calculation of the response time if the two years are found to be different between the start and end time, and the time duration is greater than four hours, the response time is set to zero.

Response Time 2

The 'Response Time 2' field that is generated also uses a start time field and an end time field to calculate a response time. The difference in the values of this numeric field is that it contains no decimal places.

Day of Week

The 'Day of Week' field is calculated in conjunction with the 'Date' type field. When the 'Date' type is selected, a check box becomes available that provides the option to calculate the 'Day of Week' field. This field contains an integer between 0 and 6 that represents which day of the week the date of the incident falls on. 0 represents Sunday, 1 represents Monday ... 6 represents Saturday.

The screenshot shows a dialog box with two tabs: 'Field Type' and 'Source Field'. The 'Field Type' tab is active. It contains the following elements:

- 'OmegaGIS Field Type': A dropdown menu with 'Date' selected.
- 'OmegaGIS Field Name': A text input field containing 'NewDate'.
- 'Create Day of Week Field': A checked checkbox.
- 'DOW Field Name': A text input field containing 'NewDOW'.

Field Name

A new name must be entered for the OmegaGIS field. If the field name is already in the dataset, or it is an OmegaGIS reserved field name or a SQL reserved word, a warning is issued to the user when the tool is run. SQL reserved words include 'Date', 'Time', 'Update' and 'Select'. Additional SQL reserved words depend upon the dataset selected. Check the ArcGIS documentation for more detail. A list of OmegaGIS reserved field names is provided below.

- iwStandard
- iwGeoName
- iwStep
- iwGeoSteps
- OmegaGIS_Source
- OmegaGIS_Count
- OmegaGIS_Density
- Omega_Difference
- Omega_Expected
- Omega_RespTime
- Omega_Station
- Omega_NetworkID

Source Field

In addition to the Field Type tab, the information on the Source Field tab must be filled out in order to move to the next step in the Field Manager. The source field identifies which field values will be used to generate the new OmegaGIS field values. The fields available in the OmegaGIS Source Field list are those fields that have a character or numeric data type in the data layer selected. When a source field is selected from the list, the 'Sample Value' textbox is populated with a sample value from the data layer. The sample value is found by searching through the first 100 records in the data for the first non-null value.

The 'Sample Value' is important in that it provides an example of the data so that a format may be selected from the 'Format' list box. The 'Format' is necessary so that the OmegaGIS Fields Manager can modify the original data into the format required by OmegaGIS routines. A 'Test' button is available in order to check quickly whether the format selected matches the data in the selected source field.

Attachment A

The elements of a date-time format are described in the table below. The delimiter for the date-time value may be any value.

Element	Description
y	year
M	month
d	day
h	hour
m	minute
s	second

A list of the supported date and time formats are shown below. The currently supported formats are the ones Omega most commonly encounters and this list will continue to grow in the future. The formats that are displayed are dependant on the field format of the source field. For example, if the source field is a numeric date field then only the 'Numeric' date formats will be displayed in the field format drop down list.

Date Formats:

Source Field Type	Format	Example
Text	yyMMdd	030131
Text	yyyyMMdd	20030131
Text	yyyy-MM-dd	2003-01-31
Text	MMddyy	013103
Text	M-dd-yy	1-31-03
Text	MM-dd-yy	01-31-03
Text	M-dd-yyyy	1-31-2003
Text	MM-dd-yyyy	01-31-2003
Numeric	yyMMdd	030131
Numeric	yyyyMMdd	20030131
Date & Text	MM-dd-yyyy hhmm	01-31-2003 1233
Date & Text	yyyy-MM-dd hh:mm:ss OR yyyy-MM-dd hh:mm:ss.sss	2003-01-31 1:33:29 2003-01-31 1:33:29.334
Date & Text	M-dd-yy h:mm:ss AM	1-31-03 1:33:29 AM

Time Formats:

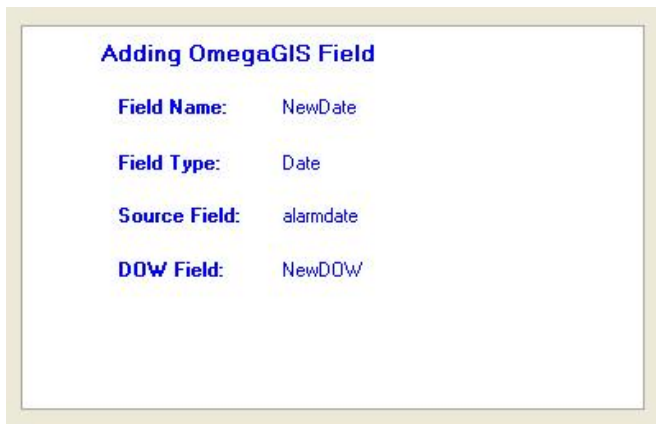
Source Field Type	Format	Example
Text	hhmm	0534
Text	hmm	534
Text	hhmmss	053428
Text	h:mm	5:34
Text	hh:mm	05:34
Text	h:mm:ss	5:34:28
Text	hh:mm:ss	05:34:28
Numeric	hhmm	0534

Attachment A

Date & Text	MM-dd-yyyy hhmm	01-31-2003 0534
Date & Text	yyyy-MM-dd hh:mm:ss	2003-01-31 05:34:28
Date & Text	yyyy-MM-dd hh:mm:ss.sss	2003-01-31 05:34:28.123
Date & Text	M-dd-yy h:mm:ss AM	2003-01-31 5:34:28 PM
Numeric	hhmmss	053428

Summary

The 'Next' button becomes available when all of the information necessary to calculating the new field has been entered. The Summary dialog is opened before the processing begins. The Summary dialog provides a review of the data that will be used to generate the new OmegaGIS Field

**Adding the New Field**

Clicking the 'Finish' button on the Summary dialog starts the data processing. The information provided is first validated to ensure that the new OmegaGIS field will contain valid data. The field name entered is checked to ensure that it is not already in the dataset. The source field selected is checked to ensure that it can be found in the dataset, the format selected is tested against the sample data to ensure the results of the processing will be valid. Finally the new field name is checked to ensure that it is not a reserved OmegaGIS field name or a reserved SQL word.

Removing an OmegaGIS Field

An OmegaGIS field can be removed from a dataset using the 'Remove OmegaGIS Field' option in the OmegaGIS Fields Manager. The field name can be selected from a list of OmegaGIS fields. Once selected, the 'Next' button moves to the Summary dialog. Clicking on the 'Finish' button removes the field from the dataset permanently.

Step 1. Select the option

Attachment A**Step 2. Select the field to remove****Step 3. Review the results and begin processing****Updating an OmegaGIS Field**

Updating an existing OmegaGIS field enables the user to change the values of the field by selecting a new source field on which the new values can be based. For 'Date', 'Time' and 'Day of Week' fields, a new source must be selected as well as

Attachment A

the format that describes the source information. Updating a 'Response Time' or 'Response Time 2' field requires that a new start source field and end source field be identified as well as their formats.

Step 1. Select the Update option



Step 2. Select the field to update



Step 3. Review the information and process field



Omega Query Editor

Saved Queries are used in Omega software to allow fast construction of the most commonly queried data attributes. The

Attachment A

queries are based on the information contained in a feature class, which links geographic data to attribute data. By storing queries for commonly used categories, queries can be quickly constructed interactively through various Omega tools and menu interfaces by simply checking off the attributes instead of entering full SQL based queries.

The role of the Omega Query Editor is to facilitate the pre-entry of SQL based queries that will be used to parse full queries in the interactive environment. It also provides tools to facilitate the import of previously used Omega_Query.MDB (used in versions of Omega software prior to version 4.0) to the new Omega_Query.ODB files.

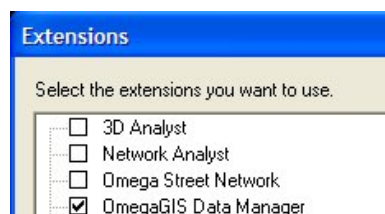
Through the use of a dynamic interactive environment, the need for previous knowledge of the underlying database structure used for Omega Saved Queries is minimized, instead saved queries can be created and ordered through the use of options menus and interactive SQL query builders. Once the queries are saved to the database, they will persist for future use in the saved query environment within Omega products.

Accessing the Omega Query Editor

The Omega Query Editor is accessed through ArcCatalog by selecting the Omega Query Editor button located on the OmegaGIS Data Manager toolbar.



The Omega Query Editor is only enabled when the OmegaGIS Data Manager extension is turned on. From the Extensions dialog in ArcCatalog, that is available from the Tools pull down menu. Check the **OmegaGIS Data Manager** extension to enable the Omega Query Editor. The OmegaGIS Data Manager requires that one of the following Omega Desktop extensions is licensed; CrimeView, FireView, School Planer or the Omega Import Wizard.



Startup Dialog

When the Omega Query Editor is opened from ArcCatalog the Startup dialog appears. This dialog provides a starting point in using the editor. There are three options:

[Create a new Omega query database](#)

Create an entirely new Omega_Query.ODB saved query database. The initial database will be empty and tools for both populating and setting database options will be available.

[Upgrade from Omega_Query.MDB](#)

Imports a legacy Omega_Query.MDB saved query database file (found with Omega Desktop products prior to version 4.0) to the new Omega_Query.ODB supported format.

[Edit existing Omega query database](#)

Opens an existing Omega_Query.ODB database for editing.

Upgrade Query Database

Omega Desktop version 4.0 includes a new format for the saved query database. This new format is required due to the new functionality that has been introduced that includes:

- Improved tools to create and edit saved queries.
- Support the display of the saved queries in columns that is required by the School Planner extension.
- Support for more query groupings; the previous release only supports two while the version 4.0 release now supports 50.
- Improved trouble-shooting tools.

Attachment A

- Future support for the file based Geodatabase that is to be released with ArcGIS 9.2.

The Omega Desktop version 4.0 can no longer use the old version of the saved query database, Omega_Query.MDB. Consequently, a [wizard](#) has been included with the Omega Query Editor that will upgrade the legacy version to the new Omega_Query.ODB. The wizard is accessible from the [Startup dialog](#).

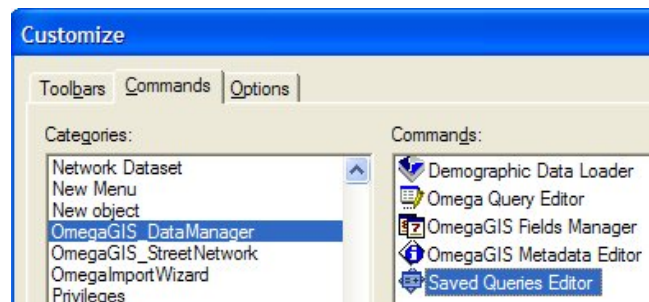
Note: There is no ability to convert the Omega_Query.ODB file that is used at version 4.0 to an older version.

Legacy Saved Query Editor

The old version of the Saved Query Editor is installed with Omega Desktop version 4.0. The button to open the editor is not added automatically to the OmegaGIS Data Manager toolbar, but can be added manually by using the Customize dialog in ArcCatalog.

Outlined below are the steps to add to the legacy Saved Query Editor to ArcCatalog.

1. Open ArcCatalog.
2. Open the Customize dialog; select the "Customize" item that is available from the Tools pull down menu.
3. Select the "Commands" tab; it may take some time for the lists to populate.
4. In the Catalogs list, select "OmegaGIS_DataManager".
5. In the "Commands" list, drag the "Saved Queries Editor" item to an existing toolbar.



Note: Omega will provide limited support to the legacy Saved Query Editor; it is recommended the new Omega Query Editor be used in its place.

Upgrade Query Database Wizard**1. Location for New Database**

Enter the path to the destination folder where the new Omega Query database will be generated. Select the folder by using the browse dialog or by typing in the path.



Once the destination folder is specified, press the [Next](#) button. When the Next button is selected, the following checks occur:

- The destination folder cannot already contain an existing Omega_Query.ODB file.
- The destination folder must exist on disk.

Tip: Omega Desktop extensions in ArcMap search for the Omega query database by default in the project workspace folder. This folder has the same name as the ArcMap document and is located in the same folder as the document.

Upgrade Query Database Wizard

2. Database to Upgrade

Omega_Query.MDB File

Use the browse button to select the Omega_Query.MDB file is to be upgraded into the destination folder selected in the previous step.

Query Groups

When a legacy query database is selected, the query groups contained in the database are loaded into the list. Select the query groups which are to be imported by checking the box. By default, all of the query groups will be selected for the import process. At least one query group must be selected in order to import the database.

To move onto the next step, select the [Next](#) button.

Upgrade Query Database Wizard

3. Summary

The final step in updating a legacy saved query database displays a summary of the information collected by the wizard.

Review the information to ensure that it is correct. If any changes need to be made, use the Back button, otherwise press the Run button to perform the [upgrade](#) operation.

Upgrade Query Database Wizard

Upgrade Processing

After the parameters have been collected from the wizard dialogs, the Omega Query Editor will upgrade the legacy saved query database to the new Omega_Query.ODB file.

Validation during upgrade

During the upgrade process, the following checks are made to ensure validity in the destination database including the following:

- Restricted characters (< > ') are replaced with the underscore character (_).
- All query group names must be under 100 characters in length.
- The query group name must not already be in use in the database (it must be unique). If it is found to already be in use, a unique name will be automatically reassigned to the query group.

Query Groupings

Previous releases of the saved query database only support two types of query groupings; primary and secondary. During the import process, these two grouping types are created and the primary is set to be the default grouping.

The primary grouping is set with a black font color and the secondary is set with a blue color in order to easily differentiate between the different query groups. These settings can be changed through the Omega Query Editor.

About Omega Query Editor

The Omega Query Editor dialog is used to edit an existing Omega query database (Omega_Query.ODB file).

There are numerous panels that are available for editing. To navigate between the panels use the lists on the left side of the dialog. The panels are divided into two main sections:

Query Database

The options that are common to the Omega query database are divided into three panels that are always enabled.

[Database](#)

Attachment A

Panel provides general information for the Omega query database and allows one to set a password.

[Query Groups](#)

This panel displays a list of all of the query groups that are contained within the database.

[Utilities](#)

The panel contains a list of utilities available for the Omega query database.

Query Group

Only one query group may be edited at a time. When editing a query group, the navigation list for the query groups is enabled. These panels have functionality that are specific to the query group being edited.

[General](#)

The panel contains information specific to the query group currently being edited.

[Reference Data](#)

Panel provides the ability to set reference to feature classes that are to be used in testing the attribute query syntax.

[Query Grouping](#)

The panel provides the ability to edit the query groupings.

[Edit Queries](#)

The panel allows one to create new saved queries or change how the saved queries are displayed to the user.

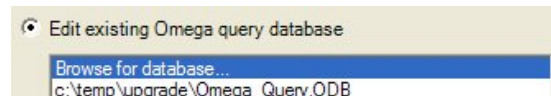
[Columns](#)

This panel provides the ability to organize the saved queries in columns.

The name of the query group that is currently being edited is provided on the status bar at the bottom of the dialog.

Edit Existing Query Database

To edit an existing Omega query database, from the [startup dialog](#) select the Edit existing Omega query database option.



There are two methods to select the Omega query database to edit:

Browse

Select the "Browse for database..." item in the list and then click the OK button. The browse dialog will open; from this dialog navigate to the Omega_Query.ODB file to edit. When the appropriate Omega_Query.ODB file is selected, click the Open button that will open the Omega Query Editor.

Recent database

Rather than browsing to an Omega_Query.ODB file, the list contains those databases that have been previously edited by the user currently logged into the computer. Up to eight databases are displayed. Only databases that are found on disk are displayed in the list.

Select a recently edited database in the list and then click the OK button to open the Omega Query Editor. Alternatively, double click the database in the list.

New Omega Query Database

A new Omega query database can be created with the wizard dialog. This dialog is accessed from the [Startup dialog](#) and the [Utility panel](#).

Outlined below are the steps in the wizard to generate a new Omega query database.

1. Location for new database

Provide the path to the folder where the new Omega query database is to be created. Either type in the path or browse

Attachment A

to the location.

The folder to create the Omega query database must exist and the folder must not already contain the Omega_Query.ODB file.

2. Summary

The final step in creating a new query database displays a summary of the information collected by the wizard. Review the information to ensure it is correct. If any changes need to be made, use the Back button, otherwise press the Run button to create the new database.

After the database has been created, the [Omega Query Editor](#) is opened.

Database Panel

The database panel provides generate information for the Omega query database and allows one set a password.

Database Description

The database description is for user defined information, such as the Omega client that database has been build for. The description is limited to 255 characters.

The description is saved to the Omega query database only when the database is saved.

Database Information

Database Version

Version of the Omega query database. Omega Desktop version 4.2 requires the Omega query database of version 4.0 or 4.1.

Omega Desktop version 4.2 ships with the Omega query database template version of 4.1. [Newly generated](#) Omega query databases use the template version 4.1. The only change with the version 4.1 template is that by default, the File Geodatabase [field qualifier](#) is used.

Date Edited

The date edited text box contains the date and time of when the last time the database has been saved.

Database Path

Path to the Omega_Query.ODB that is currently being edited.

Password Protection

A password can be set in order to prevent unauthorized use or alteration of the database. If a password is set, then the user will be prompted to enter the password whenever the Omega Query Editor is opened. If no password is entered or if an invalid password is entered, then an error will result and the Omega Query Editor will remain closed.

To set the password, click on the Set Password button. In the pop-up dialog, enter the desired password twice and press the OK button. Next time the Omega Query Editor is started, this password will need to be entered. The password must satisfy the following requirements:

- The Omega Query Editor password cannot contain any spaces.
- The Omega Query Editor password must be 20 characters or less.

A password is not required in order to use the database with client applications, just to make changes through the editor.

Query Groups Panel

A *query group* is a collection of saved queries that are used to hide the creation of SQL attribute queries from users of

Attachment A

Omega Desktop applications. A query group is registered to a feature class using the Omega Metadata Editor; this is how the Omega Desktop applications know which saved queries to display when the feature class is selected.

The Query Groups panel displays a list of all of the query groups that are contained in the database. A single Omega query database can contain up to 100 query groups.

The Query Groups panel contains the following functionality:

[New](#)
[Edit](#)
[Copy](#)
[Append](#)
[Import](#)
[Remove](#)

New

Creates a new query group in the database and starts an edit session for that new query group. A unique name for the query group is generated; the names of the query groups within the database must be unique.

Edit

For the selected query group in the list, starts an edit session. When a query group is being edited, the "Query Group" navigation items are enabled which allows for the editing of the query group.

If the Edit button is clicked and the selected query group is currently being edited, the [General panel](#) is displayed without reloading the query group information.

Copy

Entire query groups can quickly be copied from other Omega query databases (Omega_Query.ODB) by using the copy utility. When the Copy button is pressed, the Copy Query Group dialog is displayed that has the following parameters:

Omega query database

Use the browse button to select the database (Omega_Query.ODB) containing the query group to be copied.

Query group

Once the Omega query database has been selected, the list of query groups contained in the database is populated. Select the query group to be copied.

When the OK button is selected on the Copy Query Group dialog, the selected query group is automatically transferred to the current database. Once the transfer is completed, the newly copied query group is placed in an edit session.

The utility ensures that the name of the query group being imported is unique among the query groups in the database. If the name of the query group is not unique, the name is automatically renamed.

During the transfer process, a new Query ID value is generated. The Query ID value to identify the saved queries selected with both the Cyclical Reports and Threshold Alert routines.

Append

Query Groups that are stored within the same Omega query database can be appended to each other. When the Append button is pressed, the Append Query Group dialog is displayed that has the following parameters:

Source query group

The drop down list contains all of the Query Groups located within the Omega query database currently being edited. Select the Query Group to append. The selected Query Group is not altered.

Destination query group

The drop down list contains all of the Query Groups located within the Omega query database currently being edited except for the Query Group selected in the Source query group list. Select the Query Group to have saved queries appended to.

When the OK button is selected on the Append Query Group dialog, the selected source Query Group is appended to the destination Query Group. During this process, the following occurs:

- The [Query Groupings](#) from the source Query Group are copied to the destination Query Group. There is a check to ensure that the name of the query grouping is unique among the query groupings in the destination Query Group; when the name is not unique it is automatically renamed. The default query grouping in the destination Query

Attachment A

Group is not altered.

- The saved queries from the source Query Group are appended to the bottom of the existing saved queries in the destination Query Group.
- All saved queries are given a new unique Query ID value.
- Any [Query Viewer Columns](#) or [Exclude Saved Queries](#) identified in the source Query Group are not copied to the destination Query Group.
- The attribute syntax of all of the saved queries from the source Query Group are verified using the [reference data](#) of the destination Query Group.

After the append process is completed, the destination Query Group is made editable.

Import

Opens the [wizard](#) that creates a query group from a pre-existing MS Access database table.

Remove

Removes the selected query group from the Omega query database. Once removed, the query group cannot be retrieved.

Utilities Panel

The Utilities panel contains the functionality outlined below.

New Database

Opens a [wizard](#) that creates a new Omega query database.

Compact Database

Edits to the Omega query database may result in an increase of the Omega_Query.ODB file size. The "Compact Database" utility attempts to reduce the size of the Omega_Query.ODB file.

To compact the Omega query database currently being edited, select the Compact button.

Export to Web.config XML

The utility [exports](#) a single query group to an [XML file](#). The format of the query group within the XML file is the same used by Omega web applications (version 1.0).

To export a query group from the current Omega query database, select the Export button.

General Panel

The General panel contains information specific to the query group currently being edited.

[Query group name](#)

[Query Group ID](#)

[Description](#)

[Statistics](#)

[Save edits](#)

Query group name

The name of the query group can be altered. This name is registered in the metadata of the feature class for which the query group contains the saved queries for.

Before the query group information is saved to the database, there are the following checks:

- The name is 100 characters or less.

Attachment A

- A name is provided. Both the leading and trailing spaces are removed. When no name is provided, a name is automatically provided.
- Invalid characters are replaced with an underscore character "_". These characters include "<", ">" and single quotes.
- The name is unique among the query groups in the database. When the name is not unique, the query group is not saved to the database and there is a message displayed.

Query Group ID

The read-only ID for the query group. This ID used by Omega Desktop when constructing the SQL query syntax. Additionally, this ID is required for assigning query groups to a layer that is used in an Omega Server application.

Description

User defined description of the query group. The name is limited to 255 characters. When no name is provided, the word "Required" is automatically entered when the changes are saved to the database.

At the Omega Desktop version 4.0 release, the description is only seen within the Omega Query Editor.

Statistics

Statistics are displayed for the saved queries contained within the query group and are useful to get an overview of the status of the saved queries.

The statistics are calculated when the query group is first loaded and after the edits are saved to the Omega query database.

The statistics include the following information:

Total saved queries

Includes those saved queries that lack an attribute query; these are the saved queries that appear as a folder in the tree view.

Format details

For each of the supported formats, Personal Geodatabase, ArcSDE, File Geodatabase and shapefile, the number of saved queries with an attribute query and their status.

Valid - attribute query has been tested and it successfully selected at least one feature.

Warning - When the attribute query has a warning, it has either been tested and no records were selected or the attribute query has not been tested as there was no reference data to test against.

Error - There is an error with the attribute query.

No attribute query - The attribute query is missing for the format.

Save edits

All edits made to the query group are not persisted to the Omega query database until the Save button is selected. Failing to save before exiting the Omega Query Editor will result in all edits being lost.

The File pull down menu also contains a Save menu item that also saves the query group.

Reference Data Panel

Reference data is used to test the attribute query syntax while editing the saved queries.

Add Reference

To add reference to a feature class, select the browse button and then navigate to the feature class. When the feature class is selected, the following checked:

- Geometry of point.
- Valid feature class.

Attachment A

Note: The ArcGIS 9.2 release introduced the File Geodatabase. One of the changes that also occurred was that when one browses for a Personal Geodatabase feature class, one is also able to select a File Geodatabase. When adding reference to a feature class stored in a Personal Geodatabase, there is a check of the source format after the feature class is selected to ensure it is a Personal Geodatabase.

After the feature class has been referenced, the [field qualifiers](#) are updated but not whether or not to use those field qualifiers.

Remove Reference

To remove the reference to a feature class, simply click the Remove button.

Missing Reference

Adding reference to the feature class does not alter the feature class; the Omega query database only stores information on how to find the feature class. When the Query Group is opened in an edit session, reference is made to the feature classes. If the feature class cannot be found, such as when it has been renamed, there is a red exclamation mark beside the path to the workspace. The tool tip contains the information on why the feature class could not be found.

When the reference to the feature class is missing, one will not be able to open the Query Builder dialog or verify the attribute query syntax.

Field Qualifiers

The Field Qualifiers button opens the [Field Qualifiers](#) dialog.

Query Grouping

Query groupings are used in the construction of the SQL query when joining multiple saved queries. Those saved queries that have the same query grouping are joined together with the "OR" connector while different query groupings are joined with the "AND" connector.

At previous releases, Query Groups only supported two query groupings; primary and secondary. At the version 4.0 of Omega Desktop it is now possible to commit up to 50 query groups and assign a customized color to each group in order to aid in identifying the different groups when they are displayed in the tree format.

New Query Grouping

To add a new query grouping, press the New button. The bottom of the Query Grouping panel contains the details for the new query group. The following items may be edited for the query grouping:

Grouping Name

The name must be unique among all other query groupings for the query group being edited. The name must also not contain single quotes.

Text Color

The text color is used in the tree view to assist in easily identifying different query groupings. Click the color button to open the color picker dialog. This dialog is used by ArcGIS to select colors. The "No color" option is not supported; consequently when this option is selected, the text color is changed to black.

Default Grouping

One query grouping must be set to the default grouping; the first grouping created is always set as the default. When a new saved query is created in the editor, it is assigned to the default query grouping.

The edits to the query grouping details are not updated until the Apply button is selected.

Removing a Query Grouping

To remove a query grouping, select the grouping in the list and press the remove button.

When a query grouping is removed, a check is performed to determine if any saved queries have been assigned to the query grouping. Since all saved queries must be assigned to a query grouping, a new query grouping has to be assigned. This is done with a dialog that provides a list of all of the query groupings excluding the one to remove.

If the default query grouping is removed, the first query grouping in the list is set as the default query grouping.

Edit Queries

The Edit Queries panel allows one to create new saved queries or change how the saved query is displayed to the user. The saved queries are displayed in a tree on the left side of the Edit Queries panel. The details of the selected saved query node are displayed on the right side of the panel.

[View of saved Queries](#)
[Saved Query Status](#)
[Toolbar](#)
[Saved Query Details](#)

View of Saved Queries

The saved queries are displayed on the left side of the Edit Queries panel. How those saved queries are presented is based on the View. The View is controlled by the drop down list on the toolbar.



Outlined below are the different views available.

Tree View

This view displays all the saved queries in an expandable list. This view illustrates the presentation of the saved queries in Omega Desktop applications and shows a hierarchical relationship between the saved queries. Three levels of saved queries are supported.

While in the tree view, all of the functionality provided on the toolbar is available. This includes; add a new saved query, editing, cut-copy-paste and changing the location of the saved query node.

Query Grouping

In Query Grouping view, the saved queries are divided into their [query groupings](#). Although the saved queries can be edited, the saved query nodes cannot be moved or removed.

All formats - Errors & Warnings

All saved queries that have either an error or warning associated with the attribute query syntax for any of the support formats are displayed in the tree. Although the saved queries can be edited, the saved query nodes cannot be moved or removed.

When all of the issues have been resolved for a saved query, the icon of the saved query node is updated but the saved query remains in the tree until the tree is reloaded.

All formats - Errors

Displays a list of all the saved queries that have outstanding errors with the attribute query syntax for any of the supported formats. The saved queries can be edited but the saved query nodes cannot be moved or removed.

When all of the issues have been resolved for a saved query, the icon of the saved query node is updated but the saved query remains in the tree until the tree is reloaded.

Personal GDB - Errors & Warnings

Displays a list of all the saved queries that have outstanding errors or warnings associated with their Personal Geodatabase feature class attribute queries. The saved queries can be edited but the saved query nodes cannot be moved or removed.

When all of the problems with the personal Geodatabase attribute query are resolved, the icon of the saved query node is updated but the saved query remains in the tree until the tree is reloaded.

ArcSDE - Errors & Warnings

Displays a list of all the saved queries that have outstanding errors or warnings associated with their ArcSDE feature class attribute queries. The saved queries can be edited but the saved query nodes cannot be moved or removed.

When all of the problems with the ArcSDE attribute query are resolved, the icon of the saved query node is updated but the saved query remains in the tree until the tree is reloaded.

Shapefile - Errors & Warnings

Displays a list of all the saved queries that have outstanding errors or warnings associated with their shapefile feature

Attachment A

class attribute queries. The saved queries can be edited but the saved query nodes cannot be moved or removed.

When all of the problems with the shapefile attribute query are resolved, the icon of the saved query node is updated but the saved query remains in the tree until the tree is reloaded.

File GDB - Errors & Warnings

Displays a list of all the saved queries that have outstanding errors or warnings associated with their File Geodatabase feature class attribute queries. The saved queries can be edited but the saved query nodes cannot be moved or removed.

When all of the problems with the File Geodatabase attribute query are resolved, the icon of the saved query node is updated but the saved query remains in the tree until the tree is reloaded.

Personal GDB - Errors

Displays a list of all the saved queries that have outstanding errors associated with their Personal Geodatabase feature class attribute queries.

When all of the problems with the Personal Geodatabase attribute query are resolved, the icon of the saved query node is updated but the saved query remains in the tree until the tree is reloaded.

ArcSDE - Errors

Displays a list of all the saved queries that have outstanding errors associated with their ArcSDE attribute queries.

When all of the problems with the ArcSDE attribute query are resolved, the icon of the saved query node is updated but the saved query remains in the tree until the tree is reloaded.

Shapefile - Errors

Displays a list of all the saved queries that have outstanding errors associated with their shapefile attribute queries.

When all of the problems with the shapefile attribute query are resolved, the icon of the saved query node is updated but the saved query remains in the tree until the tree is reloaded.

File GDB - Errors

Displays a list of all the saved queries that have outstanding errors associated with their File Geodatabase attribute queries.

When all of the problems with the File Geodatabase attribute query are resolved, the icon of the saved query node is updated but the saved query remains in the tree until the tree is reloaded.

Saved Query Status

The saved query nodes displayed in the tree on the left side of the Edit Queries dialog have an icon that provides information on the status of the attribute query.

 **Query Group**


Name of the query group which can be edited on the [General panel](#).

 **Folder**

Saved query node that lacks an attribute query. Only level 1 and 2 saved queries can be a folder as level 3 saved queries must include an attribute query.

 **Valid Query**

The attribute query is valid. The attribute query has been tested; the query was successful and at least one feature was selected.

 **Valid Query with Warnings**

The attribute query is valid but there is a warning. The warning is issued if the attribute query has not been tested with the [reference data](#) or the attribute query was tested and no records were selected.

 **Query with Error**

The attribute query is invalid. This error occurs when the attribute query is tested and returns an error or no syntax has been provided for the format.

When the saved queries are displayed in a view that is feature class specific, such as Shapefile Errors, the status of the saved query is based on that feature class format. Otherwise, the status is based on all of the formats; the most severe status being used as the saved query node icon.

Attachment A

Toolbar

At the top of the Edit Queries panel is the toolbar that contains the following controls:

 New Saved Query


Adds a saved query to the Saved Query tree. The new saved query node is added to the same level as the currently selected node. If the selected node is the query group, or if nothing is selected, then the new node will be added as a level 1 node.

New saved queries can only be added when the Tree View is in use.

 Cut Selected Saved Query

Cuts the selected saved query node and all of its children nodes; all of the nodes remain in place until pasted. The image of the cut nodes changes so that there is a visual way of determining the affected saved queries.

The cut button is only enabled when the Tree View is in use.

 Copy Selected Saved Query

Copies the selected saved query node and all of its children nodes. When the saved query node is copied to the new location, the Query ID is changed to ensure that it is unique.

The copy button is only enabled when the Tree View is in use.

 Paste

Paste the cut or copied nodes to the new location. The new location is determined based on the selected node in the tree. The list below outlines the checks that are performed during the paste operation.

Query Group Selected

The cut or copied saved queries are pasted as a level 1 saved query and are placed at the top of an existing level 1 saved queries.

Level 1 Selected

Pastes the cut or copied saved query node as a level 2 with the selected node being the parent. The children of the pasted node are also cut or copied. Before the paste operation, there is a check to ensure the saved query node to cut or copy has no more than two levels otherwise there is an error message that prevents the operation.

Level 2 Selected

Pastes the cut or copied saved query node as a level 3 with the selected node being the parent. There is a check to ensure that the cut or copied saved query node has no children otherwise there is an error that prevents the paste operation.

Level 3 Selected

Pastes the cut or copied saved query node as a level 3 and has the same parent as the selected node. It is placed below the selected level 3 saved query node.

After the paste operation, the cut or copied node is expanded if it has children nodes and is selected. Also, the paste clipboard is cleared.

The paste button is only enabled when the Tree View is in use and there is a saved query node on the clipboard.

 Remove Saved Query

Removes the selected saved query and its children nodes.

The button is enabled when there is a selected saved query node and when the Tree View is in use.

 Move Up

Moves the selected saved query node up in the tree view; the movement is limited to the same level of the saved query.

The button is only enabled when the Tree View is in use, there is a selected saved query node and that node can be moved up.

 Move Down


Moves the selected saved query node down in the tree view; the movement is limited to the same level of the saved query.

The button is only enabled when the Tree View is in use, there is a selected saved query node and that node can be moved down.

Attachment A Move Left

Moves the selected saved query node up a level and also moves the node's children.

The button is only enabled when the Tree View is in use, there is a selected saved query node and that node is a level 2 or 3.

 Move Right

Moves the selected saved query node down a level and also moves the node's children. One of the requirements of a level 3 saved query is that it has an attribute query. Consequently, when the saved query is changed to level 3, the saved query is required to have an attribute query.

The button is only enabled when the Tree View is in use, there is a selected saved query node and that node is level 1 or 2. When the selected saved query node has children, there is a check to ensure that the children will not become an unsupported level.

 Find and Replace

Opens the [Find and Replace dialog](#) that is used to search and edit saved queries.

 Transfer Attribute Queries

Opens the [Transfer Attribute Queries dialog](#) that allows the attribute query to be copied from one format to another.

 Verify Query

Opens the [Verify Saved Queries dialog](#) that tests the attribute query syntax.

Saved Query Details

When a saved query node is selected in the tree on the left side of the Query Editor panel, the details of the saved query are displayed on the right side. These details may be edited and are only saved to the tree when the Apply button is selected.

Outlined below are the parameters that can be edited for a saved query.

Name

Name of the saved query that is limited to 100 characters. A name is required but it does not have to be unique.

Query Grouping

The list contains all of the [query groupings](#).

Query ID

The query ID uniquely identifies the saved query and is created when the saved query is first generated. The query ID cannot be edited.

Item has attribute query

When this checkbox is checked, the saved query has an attribute query. When there is no check, the saved query is only a folder and tabs at the bottom of the dialog that contain the attribute query are disabled.

Item has attribute query

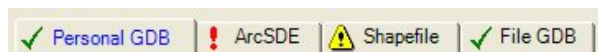
The checkbox is disabled and checked when the details of a level 3 saved query are displayed. This is the case because all level 3 saved queries must have an attribute query.

When the checkbox is unchecked, the attribute queries for all of the formats are cleared and the controls are disabled.


When the checkbox is selected again, the queries remain empty.

Attribute Query

The Omega query database currently supports four formats of saved queries; personal Geodatabase, ArcSDE, Shapefile and File Geodatabase. Each of these formats has a tab where the attribute query can be viewed and edited. The active tab has its text in blue.



Each tab has an icon before the name of the format. This icon represents the status of the attribute query for that format. Outlined below are the different status and icon:

 Valid query

Attachment A

Attribute query has been tested; it was both successful and selected at least one feature.

⚠ Valid query with warnings

Attribute query has been tested and it did not selected any records or the attribute query has not been tested; this occurs when there is no reference data for the format.

✖ Invalid query

There is an error with the attribute query.

! No attribute query

No attribute query has been provided for the format.

There are a number of tools available for creating the attribute query. These tools are accessed with buttons located on the attribute query tab. The tools are outlined below:

Error Info

When the Error Info button is selected, a message box is displayed that contains information on why the saved query had an error or warning.

The error information is created when the saved query is [imported](#) into the Omega query database or the last time the saved query was applied to the tree.

Clear

Clears the attribute query for the format.

Restore

Restores the attribute query to its state the last time the query was applied to the saved query node.

Verify

The Verify button checks the attribute query syntax and updates the icon on the tab that represents the status. The error information, accessed with the Error Info button, is not updated.

The Verify button is only enabled when the feature class for the format is [referenced](#).

Build

The Build button opens the [Query Builder](#) dialog. The button is only enabled when the feature class for the format is [referenced](#).

Apply Edits

The edits to the saved query are only persisted to the saved query node when the Apply button is selected. When the Apply button is selected, there are the following checks:

- Ensure that a name has been provided for the saved query. The name does not have to be unique. Invalid characters, which include single quotes and <> symbols, are replaced with an underscore.
- The attribute query for all of the supported formats are tested. If there is a query that has an error with the attribute query, a message box is displayed and the saved query is not persisted to the saved query node.

An attribute query can only have an error when there is reference data. If the reference data is not set for a supported format, that format will receive a warning.

If the edit to the saved query passes the validation process, the updates outlined below are made.

- The saved query node is updated with the new name.
- The saved query node icon is updated based on the status of the attribute query.
- The error information for the saved query is updated.
- The icons on the attribute query tabs are to reflect the status of the attribute queries.

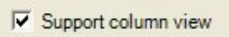
Note: The edits to the saved query are not saved to the Omega query database until the [Save button](#) is selected.

Attachment A**Columns**

The Saved Query Viewer that is used by Omega desktop applications allows saved queries to be displayed in either a tree view or a column view. Each view has similar functionality but organizes queries in a different fashion. The Columns panel is used to support the organization of the saved queries.

Query Viewer Columns

To enable the column view check the Support Column View checkbox.



The next step is to specify the level 1 saved queries whose children are to be displayed in the columns by selecting the browse button that opens the Level 1 Saved Query dialog.

The Level 1 Saved Query dialog contains all of the level one saved queries within the current Query Group. The list excludes the saved query that has been specified for the other column.

Level 3 Saved Queries

Only the children, which are level 2 saved queries, of the level 1 saved query are displayed in the columns. If there are also level 3 saved queries, these saved queries will not be visible in the columns and there is a warning displayed with the Saved Query Viewer.

Missing Reference

When the level 1 saved query that has been assigned to a column is missing there is a red exclamation mark next to the text box that contains the name of the saved query.



The missing reference can occur when the saved query is deleted or changed from a level 1 saved query. In both cases, there is a warning message after the operation.

Exclude Saved Queries: Projection Analysis

The School Planner Projection Analysis routine has specific requirements on which saved queries are to be displayed to the user. Typically, the routine requires that those saved queries that specify grade are not to be displayed.

Level 1 saved queries and their children can be excluded. Use the Add button to open the Level 1 Saved Query dialog to add the saved queries to exclude.

Field Qualifiers

Field qualifiers are used to delimit the beginning and ending of a field name in an SQL query. Field qualifiers are typically used when the field name contains spaces. Each feature class format has different field qualifiers.

Use of Field Qualifiers

The field qualifiers are used in the construction of the SQL query with the following operations:

Importing from MS Access table

The field identified as the code field uses the field qualifiers when the SQL query is automatically generated, provided that the option to use the qualifiers was selected.

Query Builder dialog

The list of the fields includes the field name and the field qualifiers when the option to use the field qualifiers is selected.

Field Qualifiers Dialog

The field qualifiers are specific to each Query Group. The field qualifiers can be edited using the Field Qualifiers dialog.

This dialog can be opened from the following locations within the Omega Query Editor:

- Reference Data panel
- Query Builder dialog

Attachment A

The Omega Query Editor contains default values for the field qualifiers. These default values are outlined in the following table:

Format	Left Qualifier	Right Qualifier
Personal GDB	[]
ArcSDE	'	'
Shapefile	"	"
File GDB	"	"

Field qualifiers are limited to a single character. When edits are made to the field qualifiers, there is a check to ensure that a value is provided.

When reference is made to a new feature class, the Omega Query Editor checks with the workspace of that feature class and updates the field qualifiers values. The option to use the field qualifiers is not altered.

Import Query Group

Query Groups can be imported from an existing MS Access table instead of being entered manually. The parameters for the import process are collected through the use of a wizard. This wizard is accessed from the [Query Groups panel](#).

The table requires the following fields:

Code

The code field contains the value that is to be searched for in the attribute query. This field can either be numeric or text. The code field is required.

Description

The description field is the text that describes the code and it is used as the name of the saved query. This field must be text or numeric and it is required.

Grouping

The grouping field is used to identify the [query groupings](#).

Query Level

A numeric field contains the level of the saved query. The valid range of values is 1 through 3.

Order By

This field identifies the order in which the records should be sorted when imported into the Omega query database.

Import Query Group

1. Query Group destination

Select the destination of the Saved Queries that are to be imported from a table in MS Access. There are two options:

New query group

When creating a new query group, provide a name. This name is limited to 100 characters and must not contain any invalid characters which include the single quote and brackets ("<", ">").

During the import process there is a check to ensure that the name of the query group is not already in use within the Omega query database. When the new name is not unique, a unique name is automatically generated.

Append to existing query group

Select the query group in the Omega query database to append the new save queries to. The new saved queries are appended to the end of the existing saved queries. If query groupings are identified, these are in addition to an query groupings that already exist. The reference data that is identified overwrites any reference data that the query group may already have.

To move onto the next step in the wizard, select the [Next](#) button.

Import Query Group

Attachment A**2. Source Database**

Use the browse button to navigate to the MS Access database (*.MDB) that contains the source data being imported. When the database is selected, select the Open button which then populates the list of tables to import.

It is not necessary for the MS Access database to be a personal Geodatabase. Any tables that begin with the "GDB_" prefix will be automatically excluded from the list of tables, as they are proprietary to the Personal Geodatabase data model.

Select the table that contains the information to import and select the [Next](#) button to continue with the wizard.

Import Query Group**3. Code and Description**

Select the field that contains the code values and the description values that are to be used to generate the saved queries. These are required fields.

Code field

The code field contains the value that is to be searched for in the attribute query. The list of code field contains both numeric and text fields. If there is a field in the table named "Code", then this field is automatically selected otherwise the first field is selected.

The field type of the code field will determine what fields are available from the reference data feature class. When the code field is numeric, only numeric fields will be able to be selected as the query field.

Description field

The description field is the text that describes the code and it is used as the name of the saved query. The list of the description fields contains both numeric and text fields. If there is a field in the table named "Description", then this field is automatically selected otherwise the first field is selected.

Note: memo fields are excluded from the list of fields.

The import operation supports forcing the code or description values to upper case. This is done by selecting the appropriate checkbox. For more complex calculations, use the tools in MS Access or ArcMap to make the updates before starting the wizard.

To move onto the next step, select the [Next](#) button.

Import Query Group**4. Order By and Query Level (Optional)****Order By**

The selection of the Order By field allows for the sorting of the saved queries when they are imported into the Omega query database. The Order By list is populated with all of the text and numeric fields that are found in the source table along with the "< None >" item that is selected by default.

When the Order By field is not used, the saved queries are imported based on how the records are stored in the table and there is no guarantee of the ordering of the saved queries. When an Order By field is identified, the saved queries are imported in ascending order (A to Z or 1 to 9).

Query Level

The Omega query database supports three levels of saved queries. The level of the saved query may be specified by selecting the Query Level field. The Query Level list is populated with all of the numeric fields that are found in the source table along with the "< None >" item that is selected by default.

When a field is selected in the list, there is a check to ensure that all of the values in the field are within the range of 1 through 3. When an invalid value is found in the field, a message box is displayed, the field is removed from the Query Level list and the "< None >" item is selected.

During the import process, there are the following additional checks:

Attachment A

- The first saved query is given the query level of 1, no matter the value specified.
- In order for a saved query to be level 3, the previous saved query must also be a level 3 or level 2. When this condition is not satisfied, the saved query is given the same level as the previous saved query.

When no Query Level field is specified, all saved queries are set to level 1.

To move onto the next step select the [Next](#) button.

Import Query Group

5. Query Grouping (Optional)

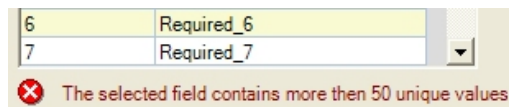
Query grouping is used in the construction of the SQL query when joining multiple saved queries. Those saved queries that have the same query grouping are joined together with the "OR" connector while different query groupings are joined with the "AND" connector. Typically, the saved queries that share the same query grouping query the same field in the feature class.

If the table being imported contains query grouping information, select the field from the list of numeric and text fields. By default the "< None >" list item is selected; no query grouping information in the table being imported.

Grouping Name

When a query grouping field is identified, the wizard populates a grid with a list of the unique values found in the table for the query grouping field. A default name of the grouping is also provided in the grid. These names can be edited by typing directly into the cell that contains the name. The name is restricted to a maximum of 50 characters and it must be unique.

When the number of unique values found in the query grouping field is greater than the maximum number supported for a query group, which is 50, then there is a warning message at the bottom of the grid and the field will not be able to be used as the query grouping field.



If appending to existing query groupings, then there is a check during the import process to ensure that the query groupings names are unique among the existing names. When an imported query group name is not unique, the import operation automatically re-assigns a new unique name.

To move onto the next step in the wizard, select the [Next](#) button. Before moving onto the next step, the following is done when a query grouping field is identified:

- Checks to ensure that the query grouping names are unique. When a name is not unique there is a warning message.
- Replaces any invalid characters (including single quote and brackets <>) with an underscore.

Import Query Group

6 - 9: Reference Data

There are four steps in the wizard where the reference data is set and field mapping is done. Each of these steps is the same except there is a single step for each of the formats of the attribute query.

Reference Data

Reference data aids in the validation of the attribute queries during the import process and is used in the field mapping. Use the browse button to select the point feature class.

Reference data is not required. When there is no reference data the query field must be manually entered.

When appending to an existing query group, the reference data selected will override the existing [reference data](#); even

Attachment A

for those formats where no reference data was selected.

Field Mapping

The grid at the bottom of the step contains a list of the query groupings along with the query field. The query field is used in the construction of the attribute query.

When no reference data has been set, the name of the query field must be manually entered. This is done by clicking in the query field cell and typing in the field name. When manually entering the field name the name is limited to 150 characters.

When the reference data has been set, the query field will contain a drop down list of the fields found in the feature class. If the field identified as the "Code" field is text, then the list of query fields is limited to those text fields found in the feature class. Conversely, the same is true when the "Code" field is numeric; only numeric fields are displayed in the list.

Field mapping:	
Query Grouping	Query Field
Schools	School_Name
Grades	Grade_Description

To move onto the next step, click the [Next](#) button. Before moving on, there is a check to ensure that a query field has been provided for each query grouping.

Import Query Group**10. Field Qualifiers**

[Field qualifiers](#) are used to delimit the beginning and ending of a field name in a SQL query. Each feature class format has different field qualifiers.

To use field qualifiers for a specific feature class format, select the checkbox. Field qualifiers are limited to a single character. When edits are made to the field qualifiers to use, there is a check to ensure that a value is provided.

When [reference](#) is made to a feature class, the wizard checks the workspaces of that feature class and updates the field qualifiers values.

To move onto the next step, select the [Next](#) button.

Import Query Group**11. Summary**

The final step in importing a query group from an existing MS Access table is a summary of the information collected by the wizard.

Review the information to ensure that it is accurate and use the Back button to make any changes otherwise press the Run button to perform the import operation.

Import Query Group**Import Processing**

After the parameters have been collected from the wizard dialogs, the Omega Query Editor will import the MS Access table as a new query group.

Saved Query Name Validation

During the import process the names of the saved queries are checked for the following:

- Ensure that a name is provided. When no name is provided, then the default name of "Required" is entered.

Attachment A

- Invalid characters, include single quotes and brackets ("<", ">"), are replaced when an underscore.

Saved Queries Editor

NOTE: The Saved Queries Editor is no longer added to the Omega Data Manager toolbar by default as this tool has been replaced with the [Omega Query Editor](#). The Saved Queries Editor is no longer being enhanced and will be removed from the installation at a future release.

The Saved Queries are shown in a [tree format](#) in the OmegaGIS routines. These queries are stored in the saved query database. This editor provides a way to create, import, and/or edit the saved queries. It is accessed from the [Omega Data Manager](#) toolbar in ArcCatalog.

When you open the **Saved Queries Editor** you will be prompted to do one of the following:

1. Create new saved queries

Start with a blank query tree and build the saved queries in the editor.

2. Import saved queries


Import saved queries from either an existing query.ini file or from an Excel template. The [Utilities](#) dialog will be opened.


3. Open existing saved queries


You will be prompted to open an existing saved query database. Then any changes can be made to the query tree using the editor.

Toolbar


The toolbar provides the following options:


-  **Add:** Select from one of the drop-down options.
 - Group:** Adds a new query group to the tree.
 - On same level:** Adds a new query on the same level as the selected query.
 - Down one level:** Adds a new query under the selected query.


-  **Edit Query:** Opens the Edit Query dialog, where queries for shapefiles, personal geodatabases, and ArcSDE geodatabases can be created and verified.


-  **Delete:** Deletes the selected query.

-  **Find:** Enter the value to find in the text box.

-  **Utilities:** Opens the [Utilities](#) dialog.

-  **Save:** Save the changes to the saved query database.

-  **Select Database:** Open an existing saved query database.

-  **Open Help:** Opens help for using this editor.

Right-Click Menu

Right-clicking on one of the queries gives the following options:

Rename: Rename the selected query.

Edit: Opens the Edit Query dialog, where queries for shapefiles, personal geodatabases, and SDE geodatabases can be created and verified.

Add: Select from one of the sub-options.

Attachment A

New Query Group: Adds a new query group to the tree.

New query on same level: Adds a new query on the same level as the selected query.

New query down one level: Adds a new query under the selected query.

Move: Select from one of the sub-options.

Up: Move a query up in the tree.

Down: Move a query down in the tree.

Query Type: Select either Primary or Secondary. By default, all queries are Primary.

Delete: Delete the selected query.

Utilities

The Utilities dialog has 3 tabs:

Password

If you would like the saved query database to be password protected, select the option here and enter the password.

This password is needed anytime the saved query database is opened in this editor. A password is not required to use the saved query database in OmegaGIS.

Verify Queries

All queries in a query group can be verified here. Select the query group and the type of queries to verify. Then select an appropriate data layer. Any problem queries found will be written to a log file.

Convert Data

The saved query database can be created one of the following ways:

1. Import from a Query.ini file. The Query.ini file was used in previous version of Omega products. This can be imported into the Excel template or the Access database. From the Query.ini file, queries for both Shapefiles and Personal Geodatabases are created. From the SDE_Query.ini file, only queries for ArcSDE are created.

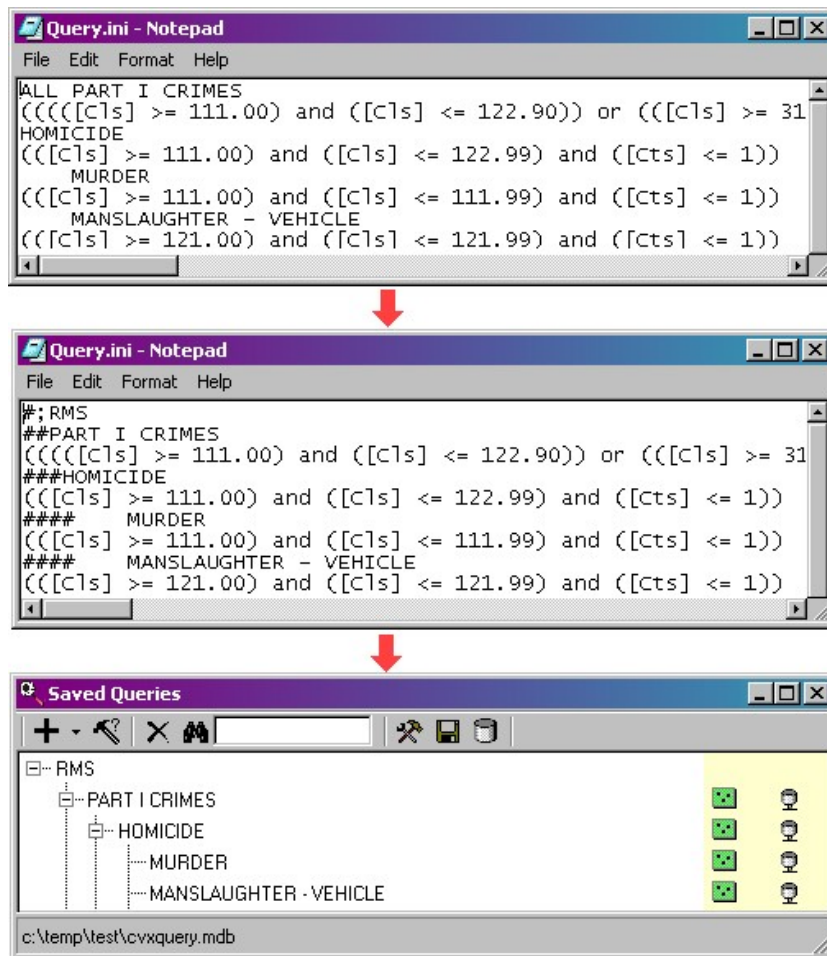
To import into the Access database, the old Query.ini file must be formatted to define the query tree levels. These are defined by adding a pound sign (#) to the beginning of each query name. The number of pound signs designates which tree level the query belongs on. The query tree can only go 4 levels deep. See Figure 1 for an example.

Using the example in Figure 1, 'RMS' is the name of the query group, which will be on the first level. The query group cannot have an associated query. On the second level under 'RMS' is the 'Part I Crimes' category. On the third level under 'Part I Crimes' are the 8 types of Part I crimes. The first one is 'Homicide' and it is further broken out into sub types 'Murder', 'Manslaughter - Vehicle', etc. These sub types are on the fourth level.

To import into the Excel template, only a valid Query.ini file is needed. If the Query.ini file has not been formatted with the pound signs, it will import all queries onto the second level. You can drag and drop the queries onto the appropriate levels. See #2 for more information.

Figure 1. Importing Query.ini

Attachment A



2. Create in the Excel template and then import into the Access database. The Excel template provides an easy way to create and edit the query tree. (See Figure 2) However, the queries created in Excel cannot exceed 255 characters. If a query is longer than 255 characters, it will be cutoff when it is imported into the Access database. Be sure to verify all queries after importing to check for any errors in the imported queries. See the Query Help worksheet in the Excel template for more information about creating queries using the Excel template.

Figure 2. Excel template

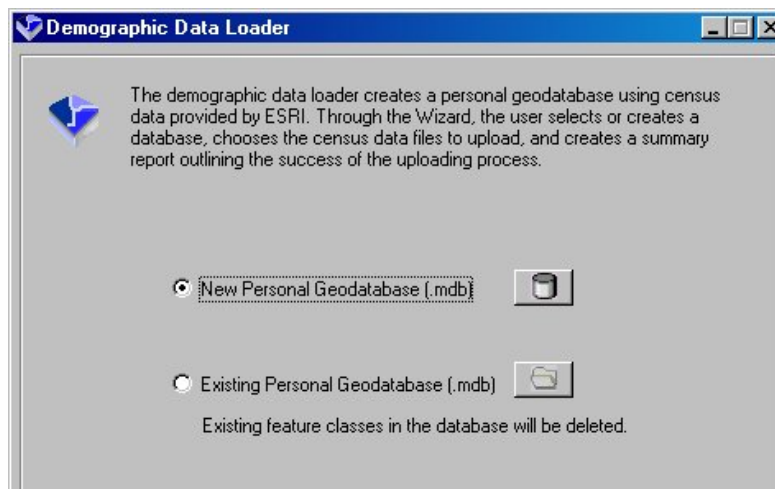
Attachment A

	B	C	D	E	F	G
1						
2	Group	Level 1	Level 2	Level 3	P/S	Query (Shapefile)
3	RMS					
4		Part I Crimes				
5			Auto Theft		1	(("Cls" >= 710.00) and ("Cls" <= 740.99) and ("Cts" <= 1))
6				Automobile	1	(("Cls" >= 710.00) and ("Cls" <= 710.99) and ("Cts" <= 1))
7				Attempt	1	(("Cls2" = "%A%") and ("Cts" <= 1))
8	RMS				1	
9		PART I CRIMES			1	
10			HOMICIDE		1	(("Cls" >= 111.00) and ("Cls" <= 122.99) and ("Cts" <= 1))
11				MURDER	1	(("Cls" >= 111.00) and ("Cls" <= 111.99) and ("Cts" <= 1))
12				MANSLAUGHTER - VEHICLE	1	(("Cls" >= 121.00) and ("Cls" <= 121.99) and ("Cts" <= 1))

3. Using this Saved Queries Editor to create or edit the query tree. The query tree can be created using the toolbar or by right clicking on any item in the query tree. Queries can be entered for Shapefiles, Personal Geodatabases, and/or ArcSDE layers, since these feature types require different query syntax. The icons on the right hand side signify which type of queries are defined.

About Demographic Data Loader

The Demographic Data Loader is used to compile source census information used by both the Demographic Viewer and the [Crime Rate Generator](#) routines. The tool creates a Personal Geodatabase (.MDB), containing the census files downloaded from the [ESRI](#) website. For information on downloading census data from the ESRI website, read about [Accessing Demographic Data](#).



To access the Demographic Data Loader, open ArcCatalog, click on the Tools menu, and select Extensions. Ensure the [Omega Data Manager](#) extension is checked. Select 'Customize' from the Tools menu; and from the Toolbars tab, choose the "OmegaGIS Data Manager".



The Omega Data Manager extension is protected from unauthorized use. At least one Omega Desktop product, such as the Omega Import Wizard, CrimeView, FireView or School Planner, must be licensed for the Omega Data Manager to be enabled.

Data Description

The Demographic Data Loader assembles census layers by joining a shapefile to a .dbf flat file. For each census boundary type (tract, block group or block), both a shapefile and flat file must exist. The shapefile contains the geographic extent for each boundary polygon in the layer. The .dbf flat file consists of the population statistics compiled by the U.S. Bureau of the Census. The files can be identified by their extensions; .shp for the shapefile, and .dbf for the flat file.

The two files are joined on a common field called STFID. If this field is missing from either file, the tables cannot join correctly. The STFID field contains values that uniquely identify each polygon in the shapefile and each record in the flat file. The shapefile consists of a record for each of the polygons making up the boundary layer. The .dbf flat file must have the associated statistical population data for each of the polygons to join correctly. In many cases, this file includes additional records that do not match any of the STFID values in the shapefile. These extra records however, have no effect on the outcome of the join, they are discarded if a corresponding polygon in the shapefile is not found.

FID	Shape	ID	FIPSSTCO	TRT2000	STFID	TRACTID
0	Polygon	1	31111	959700	31111959700	9597
1	Polygon	2	31111	959800	31111959800	9598
2	Polygon	3	31111	959900	31111959900	9599
3	Polygon	4	31111	960200	31111960200	9602

Shapefile

STFID*	POP2000	WHITE	BLACK	AMERI ES	ASIAN	HAWN PI	OTHER
31001965400	3549	3507	8	5	1	1	16
31001965500	3959	3791	11	9	72	0	59
31001965600	5432	5209	38	20	56	4	52
31001965700	1724	1559	13	12	38	1	82
31001965800	2395	2175	7	6	84	1	88

DBF Flat File

At this point in time both the Demographic Viewer and the Crime Rate Generator tools work exclusively with the census data provided by ESRI. If the Demographic Data Loader is not used to assemble this data, it is important to read through all of the information provided about the data format of the resultant census files, in order to mimic their format so that these tools can be used successfully.

Data Dictionary

Detailed information is available from both the ESRI website and the U.S. Bureau of the Census about the files used in creating geographic census information. Browse the following sites for information on the spatial reference, distance units, data accuracy and the currency of the compiled information.

ESRI: http://www.esri.com/data/download/census2000_tigerline/index.html

Census Bureau: <http://www.census.gov/main/www/cen2000.html>

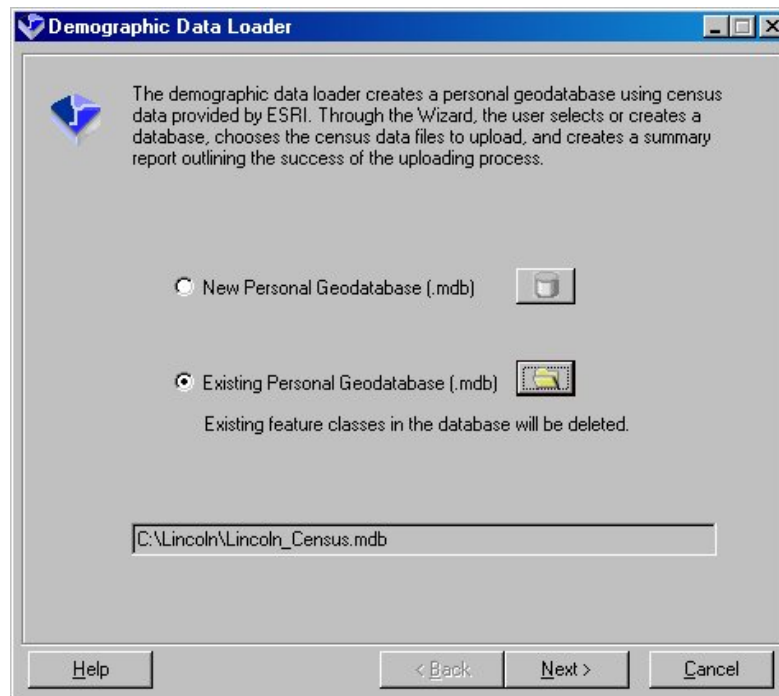
Demographic Data Loader Wizard

The Demographic Data Loader consists of a wizard made up of three dialogs. When all of the information required by the first wizard dialog is entered, the Next button becomes available, and the user may move on to the next dialog.

[Creating the Personal Geodatabase](#)
[Selecting the Census Data](#)
[Summarizing the Results](#)

Creating the Personal Geodatabase

The first dialog provides an option to either create a new personal geodatabase, or use an existing personal geodatabase. If the existing personal geodatabase is selected, any feature classes already existing in the database are deleted.

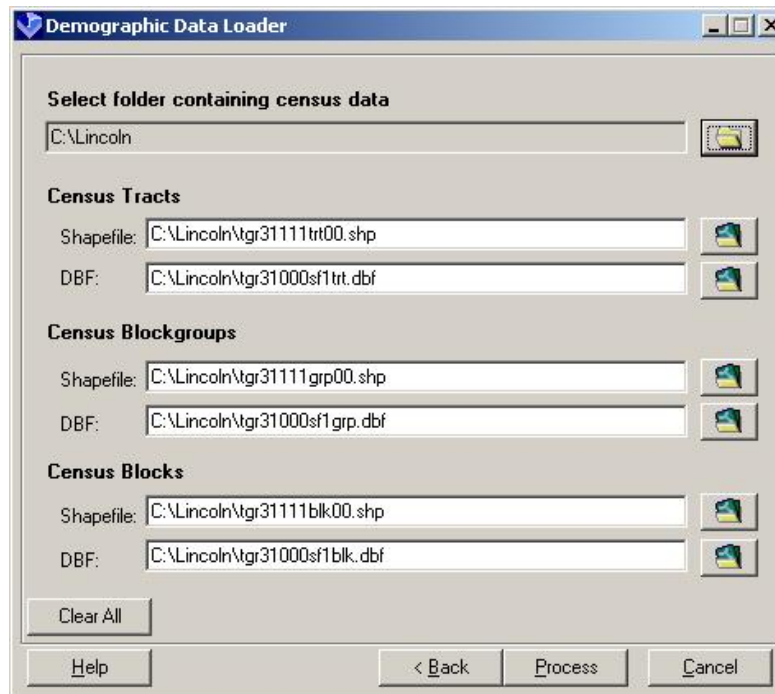


Note that at this time, only personal geodatabases may be created or updated. The File Geodatabase format introduced at ArcGIS 9.2 is not an option. If creating a new database, only a personal geodatabase will be produced. If selecting the 'existing personal geodatabase' option, a warning will occur if a file geodatabase is selected.

Selecting the Census Data

Moving on to the next dialog, if the census files are all located in the same folder, and the original names have been retained, all of the text boxes on this dialog may be updated automatically simply by choosing the folder in which the data resides. Alternatively, these file names can be browsed manually.

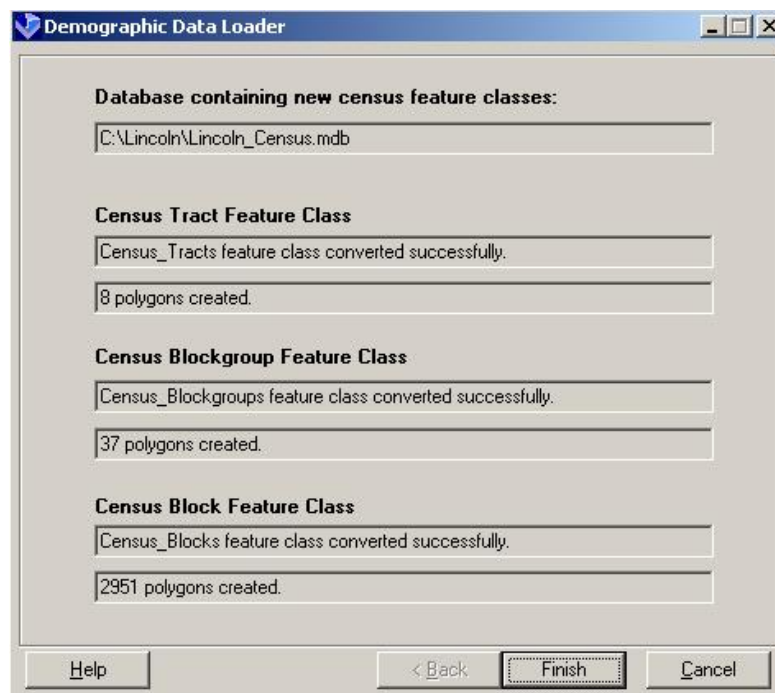
Generally, three file names are available representing the three census boundary types; tracts, block groups and blocks. The boundary files can be recognized by the file extension as well as the abbreviated names contained within the file name. For instance, *trt*, identifies census tracts, *grp*, is short for block groups, and *blk*, stands for blocks. Ensure that the correct file is placed the appropriate text box. If the incorrect files are entered, a warning will be issued on the last dialog.

Attachment A

As a reminder, census data is accessed through the ESRI website. A detailed account of this procedure can be viewed within the [Accessing Demographic Data](#) section of the Demographic Viewer help.

Summarizing the Results

The final dialog provides a summary of the success or failure of the new census layers. For each file, census tracts, census block groups and census blocks a message states whether the process succeeded or failed. If the process succeeded, the number of polygons created is identified. If for any reason during the processing an error occurs, a warning is issued. A warning can be identified by a red exclamation beside the summary information.



Getting Help

Analysis using Geographic Information Systems (GIS) can be a complex process. The Omega Desktop suite of tools, created by The Omega Group, is designed to simplify this process but questions and issues can arise. There are a number of ways to get assistance.

[Training](#)

[Product Documentation](#)

[Omega Customer Support](#)

Training

Training is an essential component in maximizing an investment in technology. There are several training options outlined below:

Omega Training

The Omega Group provides training when the Omega Desktop project is installed at the client's site. The training focuses on using the routines included with Omega Desktop.

Omega Remote Training Modules

The Omega Group offers remote follow up training to existing clients through GoToMyPC software. The remote access software allows clients to dial directly in to the Omega Project Manager's computer and work with their own application. A few topics covered by the modules include 'CrimeView', 'Administrating a Application' and 'Geocoding'. Refer to [The Omega Group's](#) web site for further information.

Omega User Training Conference

The Omega Group has an annual training conference where the user can attend workshops and labs that focus on how to use Omega products. Refer to the [Omega Group's](#) web site for the date of the next training conference.

ESRI Instructor Led Courses

Attachment A

An understanding of ArcGIS is necessary to use OmegaGIS efficiently. ESRI provides instructor led training courses in ArcGIS. Information on the different courses available can be found on the [ESRI](#) web site.

ESRI Virtual Campus

The ESRI Virtual Campus includes a series of self-pace courses that are offered through the internet. There are a wide range of courses, many of which are free. Information on the ESRI Virtual campus may be found at the [ESRI](#) web site.

Product Documentation

Omega's product documentation is a great place to find detailed information on each of the routines and tools provided with Omega Desktop. There are two important components to the documentation; the descriptions of each routine and tool, and the troubleshooting information available when a problem is encountered using Omega Desktop.

Descriptions of each Omega Desktop routine and tool are provided in the Help associated with the software. Clicking on any of the Omega Desktop Dialog Help buttons opens the Help directly associated with the routine or tool in question.

Within the Help documentation is a section called Troubleshooting. This section describes in detail the most common errors that may be encountered while using Omega Desktop software. Errors are identified by a unique number and the description that is issued during the use of the routine or tool. The Cause and Solution sections addressed for each Error are extremely informative, and should always be the first resource for problem solving when using Omega Desktop software.



Error: 7800103

There are no Feature Layers in the active data frame; unable to open OmegaGIS dialog.

Omega Customer Support

For those organizations that have a current support agreement with The Omega Group, customer support

Attachment A

is another way to get assistance.

Phone: (858) 450-2590

Toll Free: (800) 228-1059

Fax: (858) 450-0239

Email: support@TheOmegaGroup.com

Web: www.TheOmegaGroup.com

When contacting Omega customer support, have the following information available:

- Your organization.
- The Omega Product. For example CrimeView.
- Software information:
 - *Operating System.*
 - *ArcGIS version and service pack.* This information is available from the Desktop Administrator. From the Windows Start button, select All Programs -> ArcGIS -> Desktop Administrator. The ArcGIS configuration information is displayed on the right side of the dialog. ArcMap and ArcCatalog must be closed before Desktop Administrator opens.

- *Omega Desktop version, service pack and build.* The Omega Desktop Administrator applications contains this information.

NOTE:

The Omega Group can offer our highest level of support to those clients who maintain their own GoToMyPC accounts. This remote access software will allow our support staff to directly troubleshoot an application. For more information on GoToMyPC visit The Omega Group web site.

6000 to 2025: Demographic Viewer

This section contains error messages relating to the [Demographic Viewer](#).

Error 6006 Loading the Demographic Viewer Dialog

Description

"Census geodatabase cannot be opened."

Cause

The census geodatabase houses the data layers that are used with the [Demographic Viewer](#). On opening the Demographic Viewer, the table of contents is searched for census layers. The census layer found in this case has an invalid data source. The data source may have become corrupt, may now be missing or may be of the wrong data type.

Solution

Find one of the census layers in the table of contents. Ensure that the census layer data source is contained within a Personal Geodatabase (.MDB) and that the feature class is not corrupt. If all else fails, recreate the census feature classes within a new personal geodatabase using the OmegaGIS [Demographic Data Loader](#) available as an extension to ArcCatalog.

Error 6011 Loading the Demographic Viewer Dialog

Description

"Census data not found in the active data frame. Data must be registered as a census layer. Use the OmegaGIS Metadata Editor to ensure that census layers in the data frame are registered as 'Census_Block', 'Census_Blockgroup' or 'Census_Tract'"

Cause

In order to open the [Demographic Viewer](#), at least one census layer must be contained in the table of contents. The table of contents was searched for census layers, but no layers were found.

Solution

Layers in the active data frame that are classified as census layers must have the following qualities:

1. The data source must be valid.
2. The registered type must be set to 'Census'.
3. The layer must be contained in a Personal Geodatabase (.MDB).
4. The layer must have a geometry type of polygon.

Ensure that any layer in the table of contents that should qualify as a census layer follows the requirements above.

Recreate the census data using the OmegaGIS [Demographic Data Loader](#) to ensure these requirements are met.

Error 6012 Loading the Demographic Viewer Dialog

Description

"There are no layers in the active data frame."

Cause

The active data frame does not contain any valid layers. The utility cannot be opened if there are no layers in the table of contents.

Solution

Add the census layers from the Personal Geodatabase (.MDB) that houses the census data to the table of contents.

Error 6014 Selecting a new Census Layer in the Demographic Viewer**Description**

"Census layer not found in TOC."

Cause

The census layer selected in the Demographic Viewer Census layer list box has been removed from the project, or is corrupt.

Solution

Close the [Demographic Viewer](#) and re-import the census layer into the project.

Error 6016 Creating a New Census Layer in the Demographic Viewer**Description**

"The selected field was not created in the new census shapefile. The field checker may have modified this field name to accommodate the 10 character maximum width of shapefiles. Change the field name

Attachment A

to continue."

Cause

The new layer that is created by the Demographic Viewer is a shapefile. Shapefiles have a 10 character limit on the field name. When the new layer is created, the fields from the source file are run through a field checker. The field checker automatically shortens any fields over 10 characters. If in shortening the field names, duplicate fields are created, the field checker renames the duplicate field.

For example, if the fields ObjectID_12 and ObjectID_1 are contained in the same feature class, the field ObjectID_1 is changed to ObjectID_2 after being run through the field checker. Changing the field name creates a problem because in generating the new layer, if the calculations were supposed to be based on the field ObjectID_1, it no longer exists.

Solution

This problem does not occur if the census data provided by ESRI is used and is compiled using the OmegaGIS [Demographic Data Loader](#). Recreate the data using this utility available as an extension to ArcCatalog. To avoid recreating the data, open the feature class in ArcCatalog, and rename any fields over 10 characters in length before using the Demographic Viewer.

Error 6020 Loading the Demographic Viewer**Description**

"No fields found to populate the field selection list"

Cause

Although the census layer in the table of contents may contain fields, they may not be valid for display in the field list on the Demographic Viewer dialog. If the routine does not find any valid fields, for the census layer found in table of contents, the utility will not be available.

Solution

In order to be included in the field list, a field must be numeric and cannot be an area or length field. In addition, the following fields that occur in the census data provided by ESRI are not included as they do not create viable results with the Viewer:

- Med_age Median Age
- Med_age_M Median Age Male
- Med_age_F Median Age Female
- Avg_hh_sz Average household size
- Avg_fam_sz Average family size
- Hse_Units Household units

- Rural
- Urban
- Vacant

- ID

The Demographic Viewer is designed to work exclusively with ESRI Census Tiger Line files. Download the census data from the [ESRI](#) website, and compile the data using the OmegaGIS [Demographic Data Loader](#) available as an extension to ArcCatalog.

7000 to 7025: Crime Rate Generator.

The error numbers in this section are for the [Crime Rate Generator](#).

Error 7001 Loading Crime Rate Generator

Description

"There are no layers in the active data frame. CrimeRate Generator is unavailable."

Cause

The project does not have any layers in the active data frame.

Solution

Crime Rate Generator is based on layers that contain incidents of crime and census layers containing the boundaries on which the statistics are based. If no layers exist in the data frame, the Crime Rate Generator utility is disabled as there is no data to analyze.

Error 7002 Loading Crime Rate Generator**Description**

"Census data not found in the active data frame. Data must be located in a personal geodatabase and must be registered with a 'census' metadata tag. Crime Rate Generator is unavailable." "Census data not found in the active data frame. Data must be registered as a census layer. Use the OmegaGIS Metadata Editor to ensure that census layers in the data frame are registered as 'Census_Block', 'Census_Blockgroup' or 'Census_Tract'."

Cause

Census data may appear to be in the table of contents, however if it is missing the criteria of a census data layer, it is not considered census data.

Solution

Ensure that for each of the layers considered to be census data, the following criteria is met:

1. The layer must have a registered type of 'Census_Tract', 'Census_Blockgroup' or 'Census_Block'. The registered type can be set using the [OmegaGIS Metadata Editor](#), available in the Omega Data extension in ArcCatalog.
2. The datasource of the layer must be valid. A red exclamation mark indicates an invalid data source.

3. The layer must have a geometry type of polygon.

Error 7003 Loading Crime Rate Generator

Description

"Incident layers not found in the data frame. CrimeRate Generator is unavailable."

Cause

On loading Crime Rate Generator, the table of contents was searched for layers identified as incident layers, but none were found.

Solution

Identify the layers in the table of contents that should be classified as incident layers. Ensure that the following criteria is met for each layer so that it can qualify as an incident layer.

1. The layer must be a feature layer.
2. The layer must have a geometry type of point.
3. The data source of the layer must be valid.
4. If 'Use Registered Types' is selected in the [OmegaGIS Setup](#) database, the layer must be registered as one of the selected types.
5. If 'Exclude layers created by OmegaGIS...!' is selected in the OmegaGIS Setup database, the layer must not have been created by an OmegaGIS routine.

Error 7012 Opening Census Personal Geodatabase in Crime Rate Generator

Description

"Census geodatabase cannot be opened. The file is not longer accessible or has been removed."

Cause

The Census personal geodatabase is either invalid or corrupt.

Solution

Recreate the personal geodatabase using the OmegaGIS [Demographic Data Loader](#) available in the Omega Data extension within ArcCatalog.

Error 7019 Locating Selected Incident Layer in Crime Rate Generator

Description

"Incident layer not found in TOC. Close form to reset layers."

Cause

The table of contents was searched for the incident layer selected on the dialog but was not found. The layer has either been removed, renamed or is invalid.

Solution

Close the Crime Rate Generator dialog to refresh the layer list. Re-open the dialog and select an incident layer from the list. Do not modify the names, or sources of the layers in the table of contents while the Crime Rate Generator dialog is open.

Error 7020 Locating Selected Census Layer in Crime Rate Generator

Attachment A**Description**

"Census layer not found in TOC. Close form to reset layers."

Cause

The table of contents was searched for the census layer selected in the Crime Rate Generator dialog but was not found. The layer has either been renamed, removed or is invalid.

Solution

Close the Crime Rate Generator dialog to refresh the layer list. Re-open the dialog and select a census layer from the list. Do not modify the names, or sources of the layers in the table of contents while the Crime Rate Generator dialog is open.

Error 7022 Applying Attribute Query in Crime Rate Generator**Description**

"Attribute query error. Ensure attribute query in query tree is compatible with incident layer."

Cause

The attribute query selected from the [Saved Queries Tree](#), or the query created by the Query Editor is incorrect. The syntax is invalid.

Solution

Select the query from the Saved Query Tree. Use the Edit button to open the Query Editor. Click the Verify button. If the query is unsuccessful it may be modified using the editor to create the correct syntax. The new syntax should be updated in the Omega_Query.mdb database where the saved queries are stored.

Error 7024 Field Name Changed in Crime Rate Generator

Attachment A**Description**

"The field was not found in the new census feature class. The field name may have been changed by the field checker when it was reduced to 10 characters to accommodate the maximum field width of shapefiles. The field name must be changed to continue."

Cause

The result of the [Crime Rate Generator](#) analysis is a new census layer that contains crime rate statistics. The new layer is created as a shapefile while the format is based on the layer selected from the census personal geodatabase. During the creation of the layer, a field checking process ensures that all fields are within 10 characters in width, and there are no field name duplications. In doing so, field names are sometimes renamed to accommodate this criteria.

If a field name selected on the dialog, happens to be changed due to this process, Crime Rate Generator will not continue.

Solution

Crime Rate Generator is designed to work exclusively with census data downloaded from ESRI and compiled with the OmegaGIS [Demographic Data Loader](#). Since a standardized file format is required, it is recommended that any census files used for Crime Rate Generator be created using this utility. If the tool is not used, field issues can be avoided by ensuring that all field names within the census layers are unique and within 10 characters in length.

Error 7025 Loading the Crime Rate Generator**Description**

"No population fields found for census layers. Crime Rate Generator is unavailable."

Cause

A census layer was found, but it did not contain any fields that can be displayed in the Crime Rate Generator.

Solution

Attachment A

In order to be displayed in the Population field list box in Crime Rate Generator, a population field must meet the following criteria:

1. The field must be numeric.
2. The field must not be an area or length field.
3. The field cannot have the 'objectID' field type.

In order to be included in the field list, a field must be numeric and cannot be an area or length field. In addition, the following fields that occur in the census data provided by ESRI are not included as they do not create viable results with the Crime Rate Generator:

- Med_Age
- Med_Age_M
- Med_Age_F
- Ave_hh_sz
- Ave_fam_sz
- Hse_Units
- Rural
- Urban
- Vacant

To create a census database with a standardized format that can be used by Crime Rate Generator, visit [ESRI's](#) website, download the census data, and then create the database using the OmegaGIS [Demographic Data Loader](#), available in the Omega Data extension in ArcCatalog.

9000 to 9010: Demographic Data Loader

The error numbers in this section are from the [Demographic Data Loader](#).

Error 9000 Creating a New Database

Description

"Database name already exists. Create new database name."

Cause

A personal geodatabase of the same name as that entered already exists in the folder selected.

Solution

Create the personal geodatabase in a different folder or use a different name to ensure that a duplicate database name is not created.

Error 9003 Overwriting a Personal GeoDatabase

Description

"Overwriting database is unavailable on 'create new database' option"

Cause

Access to the database is limited. Overwriting the database is unavailable.

Solution

Create a new database instead of overwriting the existing geodatabase.

Error 9004 File Validation

Description

"After the OK button is clicked, the Data Loader issues a warning message that the shapefile join field is not found."

Cause

The shapefile must contain a join field called 'STFID', if this field is missing, a warning message is issued.

Solution

Download the shapefile from the ESRI website again and ensure that the STFID field is within the attribute table of the shapefile.

Error 9005 File Validation

Description

"Dbase join field not found."

Cause

The dbase file must contain a join field called 'STFID', if this field is missing, a warning message is issued.

Solution

Download the dbase file from the ESRI website again and ensure that the STFID field is within the attribute table.

Error 9006 File Validation

Description

"Join fields are of different types. Cannot join tables"

Cause

Both the shapefile and the dbase file must contain a field called STFID in order to be joined. In addition, the field types of these files must be the same for the join to be successful.

Solution

Download both the shapefile and dbase files again from the ESRI website. If the data is downloaded properly, both of these fields should exist in the correct format.

10000 to 10050: Exception Reporting

This section contains error messages for [Exception Reporting](#) and the [Exception Report Viewer](#).

Error 10008 Creating the Exception Report Table

Description

"Join Field not found in layer. Exception Reporting cannot continue"

Cause

The boundary layer field selected on the dialog when selecting boundaries by field value, is used to group the crime statistics for the final map layer. During the processing of the Exception Report, this field was not found in the boundary layer.

Solution

Close and re-open the Exception Reporting dialog. Select the boundary layer, and the 'By Field Value' option. The fields are refreshed when the dialog is opened again.

Error 10009 Loading the Exception Reporting Viewer

Description

"Exception reporting database not found. Run an Exception Report before attempting to use the Viewer."

Occurs when opening the Exception Reporting Viewer.

Cause

Exception Viewer is used to view the results of the Exception Reporting routine. When Exception Reporting is run an Exception Reporting database is created in the \Analyses project workspace. The error is due to the fact that this database is missing.

Solution

Run an Exception Report routine before trying to open the Viewer. Exception Reporting is available from the Analysis button on the OmegaGIS Main Menu.

Error 10016 Loading the Exception Reporting Viewer**Description**

"No datasets found in the exception reporting database. Run Exception Report routine to create datasets to view in the Exception Report Viewer."

Occurs when opening the Exception Reporting Viewer.

Cause

The Exception Report database does not contain any feature classes on which to base new Exception Viewer layers.

Solution

Run an Exception Report routine before trying to open the Viewer. Exception Reporting is available from the Analysis button on the OmegaGIS Main Menu.

Error 10017 Loading the Exception Report Viewer

Description

"Cannot find ERViewer.xsl stylesheet in installation folder. Cannot continue."

Occurs when opening the Exception Reporting Viewer.

Cause

The ER_Viewer.xsl file is required to view the metadata about each Exception Report available to the Viewer. The file was not found when loading the Viewer.

Solution

Search the \program files\omegagis\desktop\style folder for the file er_viewer.xsl using Windows Explorer. If the file is missing contact The Omega Group to receive a replacement file.

Error 10019 Running the Exception Report

Description

"The boundary layer is missing from the XML tag. Cannot load previous boundary selection."

Cause

To run an Exception Report routine, settings selected on the dialog are written to the project XML document. This error indicates that the process was interrupted and the boundary layer information was not copied to the file.

Solution

Re-open the dialog and run the routine again. If the project XML document has become corrupted, and the routine still does not run, go to the project workspace, and delete the project XML file from disk. This file is automatically created each time an OmegaGIS routine is run. The project XML file is identified by a name similar to MyProject.XML.

Error 10020 Validating Exception Report Selections

Description

"The current incident layer is missing from the XML tag. Cannot load current incident layer selection."

Cause

To run an Exception Report routine, settings selected on the dialog are written to the project XML document. This error indicates that the process was interrupted and the current incident layer information was not copied to the file.

Solution

Re-open the dialog and run the routine again. If the project XML document has become corrupted, and the routine still does not run, go to the project workspace, and delete the project XML file from disk. This file is automatically created each time an OmegaGIS routine is run. The project XML file is identified by a name similar to MyProject.XML.

Error 10021 Validating Exception Report Selections

Description

"The previous incident layer is missing from the XML tag. Cannot load previous incident layer selection."

Cause

To run an Exception Report routine, settings selected on the dialog are written to the project XML document. This error indicates that the process was interrupted and the previous incident layer information was not copied to the file.

Solution

Re-open the dialog and run the routine again. If the project XML document has become corrupted, and the routine still does not run, go to the project workspace, and delete the project XML file from disk. This file is automatically created each time an OmegaGIS routine is run. The project XML file is identified by a name similar to MyProject.XML.

Error 10022 Validating Exception Report Selections

Description

"There are no boundaries selected in the XML tag. Cannot load boundary selections."

Cause

To run an Exception Report routine, settings selected on the dialog are written to the project XML document. This error indicates that the process was interrupted and the boundaries on which to perform the analysis were not copied to the file.

Solution

Re-open the dialog and run the routine again. If the project XML document has become corrupted, and the routine still does not run, go to the project workspace, and delete the project XML file from disk. This file is automatically created each time an OmegaGIS routine is run. The project XML file is identified by a name similar to MyProject.XML.

Error 10024 Validating Exception Report Selections

Description

"A new layer name is missing from the XML tag. Cannot load the new layer name selection."

Cause

To run an Exception Report routine, settings selected on the dialog are written to the project XML document. This error indicates that the process was interrupted and the name for the new layer was not copied to the file.

Solution

Re-open the dialog and run the routine again. If the project XML document has become corrupted, and the routine still does not run, go to the project workspace, and delete the project XML file from disk. This file is automatically created each time an OmegaGIS routine is run. The project XML file is identified by a name similar to MyProject.XML.

Error 10026 Symbolizing New Layer

Description

"Defaultlegend.lyr file does not exist in the installation folder. Cannot continue."

Occurs when using the [Exception Reporting Viewer](#).

Cause

A default legend file called DefaultLegend.lyr is used to create the symbology for the new layer. The file should be located in the c:\program files\omegagis\desktop\symbology folder. This message is issued when the file has been removed from this folder.

Solution

Contact your project manager to obtain a new copy of this file.

Error 10027 Selecting an Attribute Query

Description

"A query is not selected. Select a query to continue or use Cancel to exit."

Cause

The Saved Query dialog is open to add a new query to the query list, but the OK button was pressed before a new query was selected.

Solution

Select a query before trying to return to the main Exception Reporting dialog, or use the 'Cancel' button to exit the form.

Error 10028 Creating the Project XML Metadata

Attachment A**Description**

"Boundary layer does not have an objectID field or the layer is corrupt."

Cause

The project XML file contains the settings selected on the Exception Reporting dialog that will be used to create the new map layer and report. The boundary layer selected for analysis was checked for an Object ID field, but the field does not exist in the layer. The ObjectID field is a required field that is created when the feature class is created. The field is used to uniquely identify features within the layer.

Solution

Right click on the boundary layer name selected and ensure that the layer has an ObjectID field. If the field does not exist, the layer cannot be used by the Exception Reporting routine.

Error 10031 Opening the Exception Report**Description**

"The Exception Report cannot be opened. Check that it exists in the \reports folder; is a valid Crystal Report, and uses data in a table within a personal geodatabase."

Occurs when the Exception Report is opened from the Exception Report Viewer.

Cause

An error exists with the Exception Report, and the report cannot be opened. The file may be corrupt, missing, or based on data that is not located in a personal geodatabase or not linked correctly.

Solution

Use Crystal Reports to open the report. Update the link to the data if necessary.

Error 10035 Validating the Exception Report Layers

Attachment A**Description**

"The boundary layer is no longer valid. Restart the routine to refresh."

Cause

The table of contents was searched for the boundary layer selected on the dialog but was not found. The layer has either been removed, renamed or is invalid.

Solution

Close the Exception Reporting dialog to refresh the layer list. Re-open the dialog and select a boundary layer from the list. Do not modify the names, or sources of the layers in the table of contents while the Exception Reporting dialog is open.

Error 10036 Validating the Exception Report Layers**Description**

"The previous incident layer is no longer valid. Restart the routine to refresh."

Cause

The table of contents was searched for the previous incident layer selected on the dialog but was not found. The layer has either been removed, renamed or is invalid.

Solution

Close the Exception Reporting dialog to refresh the layer list. Re-open the dialog and select an incident layer from the list. Do not modify the names, or sources of the layers in the table of contents while the Exception Reporting dialog is open.

Error 10037 Validating the Exception Report Layers**Description**

"The current incident layer is no longer valid. Restart the routine to refresh."

Cause

The table of contents was searched for the current incident layer selected on the dialog but was not found. The layer has either been removed, renamed or is invalid.

Solution

Close the Exception Reporting dialog to refresh the layer list. Re-open the dialog and select an incident layer from the list. Do not modify the names, or sources of the layers in the table of contents while the Exception Reporting dialog is open.

Error 10038 Loading the Exception Report Routine**Description**

"No incident layers found in the active data frame. Exception reporting is unavailable."

Cause

On loading Exception Reporting, the table of contents was searched for layers identified as incident layers, but none were found.

Solution

Identify the layers in the table of contents that should be classified as incident layers. Ensure that the following criteria is met for each layer so that it can qualify as an incident layer.

1. The layer must be a feature layer.
2. The layer must have a geometry type of point.
3. The data source of the layer must be valid.

Attachment A

4. If 'Use Registered Types' is selected in the OmegaGIS Setup database, the layer must be registered as one of the selected types.

5. If 'Exclude layers created by OmegaGIS...' is selected in the OmegaGIS Setup database, the layer must not have been created by an OmegaGIS routine.

Error 10039 Loading the Exception Report Routine**Description**

"No boundary layers found in the active data frame. Exception reporting is unavailable."

Cause

On loading Exception Reporting, the table of contents was searched for polygon layers but none were found.

Solution

Exception Reporting is based on boundary layers that form the geographic area used in the analysis. A boundary layer is classified as a layer with polygon geometry, and a valid data source. Add boundary layers to the project in order to load the Exception Reporting routine.

Error 10040 Adding Query to Query List**Description**

"Crime query is no longer valid for selected layers. Delete query to continue."

Cause

Each crime query stored in the listview has a syntax attached. The syntax is related to the layer type, and is created when the query is added to the list. If the layer type has changed in any way, making the sql syntax invalid, this message appears.

Solution

The query is no longer valid for the layer. Remove the query from the list, and recreate the query using the 'Add' button.

Error 10041 Creating a Selection of Boundary Polygons**Description**

"Selection field not found in boundary table."

Cause

The boundary layer field selected on the dialog when selecting boundaries by field value, is used to group the crime statistics for the final map layer. During the processing of the Exception Report, this field was not found in the boundary layer.

Solution

Close and re-open the Exception Reporting dialog. Select the boundary layer, and the 'By Field Value' option. The fields are refreshed when the dialog is opened again.

Error 10042 Opening the Summary Dialog**Description**

"The stylesheet used to display summary information about the routine is missing. The file Omega_exsum.xsl must be located in the installation folder to continue."

Cause

The stylesheet file called Omega_excsum.xsl is used to display information in the Summary dialog when a routine is run. If this file is missing from the OmegaGIS installation folder, an error occurs.

Solution

This file is installed when OmegaGIS is installed. If the file is missing from the c:\program files\omegagis\desktop\style folder, contact The Omega Group for a new file.

Error 10045 Searching for the Exception Report Template

Description

"The installation folder containing the exception report is missing. Ensure that the folder 'c:\program files\omegagis\desktop\reports\exception.rpt exists."

Cause

The Crystal Report template delivered with OmegaGIS called Exception.rpt has been deleted from the OmegaGIS installation folder.

Solution

In order to display Exception Report results in a report, the Crystal Report template called Exception.rpt must exist in the installation folder c:\program files\omegagis\desktop\reports. Contact The Omega Group for a copy of this report if it is missing from the folder.

Error 10048 Validating the Selected Features

Description

"SQL syntax error. The values for the query do not exist in the query database."

Cause

Saved queries are generated by creating SQL syntax for each feature class type that may be included in a project. Common feature types include: shapefile, personal geodatabase, or ArcSDE. Each type has a unique SQL syntax that is used to query features. If the syntax required for the layer selected for the analysis is missing, this error is generated.

Solution

Check the data source of the layer in question. Open the Saved Query database using the Saved Queries editor. Ensure that the SQL syntax required for the data type is included in the Saved Queries database.

Error 10049 Loading the Exception Report Viewer

Description

"Error opening the ExceptionData.mdb file. Ensure ArcCatalog is closed and restart ArcMap."

Occurs when opening the Exception Reporting Viewer.

Cause

The Exception Reporting database called ExceptionData.mdb is open in ArcCatalog. The Exception Report Viewer cannot load successfully with the database open.

Solution

Close ArcCatalog and restart ArcMap to reset the database.

Error 300110 Opening the Exception Report

Description

"Could not find the Exception Report."

Cause

The Exception Report that is opened when the checkbox is selected on the dialog is based on a file called Exception.rpt. This file could not be found by the Exception Viewer.

Solution

The Exception.rpt file must be placed in the project \reports folder in order for the Exception Viewer to find this file. If the file is missing, copy the file from c:\program files\omegagis\desktop\reports. and place in the project \reports folder.

11000 to 11010: Metadata Editor

This section contains the error messages for the [Metadata Editor](#).

Error 11000 Loading the Metadata Editor Dialog

Description

"An error has occurred loading the selected layer. The layer may be corrupt. Metadata Editor is unavailable for this layer."

Cause

The layer may be corrupt.

Solution

Recreate the layer to allow the [Metadata Editor](#) access to the stored metadata for the layer.

Error 11002 Using the Add Button on Reports

Description

"Report name already exists in list. Cannot add report name."

Cause

The report name is already contained within the list. Duplicate report names are not possible.

Solution

Change the name of one of the reports to a unique name.

Error 11003 Opening the Saved Query Database

Attachment A**Description**

"Error opening the query database. Ensure a valid query database is selected to continue."

Cause

The Query Database is invalid. Either the format of the database is incorrect, or the database has become corrupt.

Solution

Ensure a valid query database is selected to continue.

Error 11004 Opening the Metadata Editor**Description**

"The OmegaXSL stylesheet is not in the installation folder. The file must be installed in the following directory: * to be installed"

Cause

The OmegaGIS.xsl file provided in the c:\program files\omegagis\common\style folder is missing.

Solution

Contact The Omega Group to obtain a new OmegaGIS.xsl file.

Error 11005 Saving the Metadata Settings**Description**

"Write permissions are unavailable for this account. See the database administrator to update the metadata."

Cause

The dataset selected is stored in ArcSDE and the connection used to access the dataset lacks write permissions.

Solution

Have the database administrator change the permissions on the layer, or have the database administrator add the metadata revisions.

13000 to 13010: Statistical Profiler

This section contains error messages for the [Statistical Profiler](#).

Error 13001 Loading Statistical Profiler Dialog

Description

"There are too many shp_map shapefiles in the \analyses project folder. Clean up files to continue."

Cause

If a layer type is selected as the output format for the statistical profile, a new shapefile is created in the project workspace \Analyses folder called spa_map* (where * is a number). The way in which the layer name is created is by iterating through the list of file names already created in the folder, and finding the next available file number. If after iterating fifty times looking for a new filename, one is not found, this error is issued.

Solution

Open [OmegaGIS Setup](#) and select the General category. Click on the 'Project Clean Up' button to clear out the \Analyses folder of all of the shapefiles that are currently not used in the project. Aside from the \Analyses folder, the 'Project Clean Up' button also cleans all OmegaGIS folders that contain files that are not in the current project.

Error 13005 Loading Statistical Profiler Dialog

Description

"An OmegaGIS date and time field must exist to run the date-time profiler."

Cause

The Date-Time profiler is based on OmegaGIS fields created in the layer. An OmegaGIS date or time field was not found.

Solution

Use the OmegaGIS [Metadata Editor](#) available in the OmegaGIS Data Management Extension in ArcCatalog to check that the layer contains OmegaGIS fields. Create new OmegaGIS fields using the OmegaGIS Fields Manager, also available from the OmegaGIS Data Management Extension in ArcCatalog.

Error 13006 Selecting a Layer for the Statistical Profiler

Description

"The layer selected is no longer valid. Reopen the dialog to refresh valid layer list."

Cause

The layer was either removed or renamed in the table of contents, after the Statistical Profiler dialog was opened.

Solution

Close the Statistical Profiler dialog and re-open. The layer list is refreshed, excluding any invalid layers. Do not modify the table of contents while using the Statistical Profiler dialog.

Error 13007 Running the Statistical Profiler

Description

"No geocoded features were found within the recordset. Statistical profiler cannot be run."

Cause

The data selected for the analysis does not contain any geocoded points.

Solution

The data may exist in the table, but it was not geocoded. The Statistical Profiler can only run on geocoded features.

14000 to 14015: Spatial Trend Analysis

This section outlines the errors messages with [Spatial Trend Analysis](#).

Error 14000 Checking the Spatial Analyst Extension

Description

"Cannot Find Spatial Analyst License."

Cause

[Spatial Trend Analysis](#) requires the Spatial Analyst license. On searching for the license to open the routine, the license could not be found.

Solution

Spatial Analyst is an extension to ArcGIS, and must be installed and licensed separately. To check whether the extension is installed, click on the Tools menu item in the ArcMap toolbar. Select 'Extensions' and ensure Spatial Analyst exists in the list. If the extension is listed, ensure it is

selected.

If the extension is missing, or the license is invalid, use the ArcGIS CD to re-install Spatial Analyst, and license the software.

Error 14001 Checking the Spatial Analyst Extension

Description

"Spatial Analyst License is unavailable."

Cause

Spatial Trend Analysis requires the Spatial Analyst license. On searching for the license to open the routine, the license could not be found.

Solution

Spatial Analyst is an extension to ArcGIS, and must be installed and licensed separately. To check whether the extension is installed, click on the Tools menu item in the ArcMap toolbar. Select 'Extensions' and ensure Spatial Analyst exists in the list. If the extension is listed, ensure it is selected.

If the extension is missing, or the license is invalid, use the ArcGIS CD to re-install Spatial Analyst, and license the software.

Error 14002 Checking the Spatial Analyst Extension

Description

"Spatial Analyst License is available, but is disabled."

Cause

Attachment A

[Spatial Trend Analysis](#) requires the Spatial Analyst license. The license is installed but is disabled.

Solution

To enable the Spatial Analyst extension, click on the Tools menu item in the ArcMap toolbar. Select 'Extensions' and ensure Spatial Analyst exists in the list. If the extension is listed, ensure it is selected.

Error 14003 Checking the Spatial Analyst Extension**Description**

"Could not find Spatial Analyst extension."

Cause

Spatial Analyst is not licensed.

Solution

Spatial Analyst is an extension to ArcGIS, and must be installed and licensed separately. To check whether the extension is installed, click on the Tools menu item in the ArcMap toolbar. Select 'Extensions' and ensure Spatial Analyst exists in the list. If the extension is listed, ensure it is selected.

If the extension is missing, or the license is invalid, use the ArcGIS CD to re-install Spatial Analyst, and license the software.

Error 14008 Selecting a boundary layer in Spatial Trend Analysis**Description**

"The boundary layer selected is no longer valid. Restart routine to refresh."

Cause

The boundary layer selected as the geographic layer for analysis has most likely been removed from the project, or is no longer valid.

Solution

Ensure that the boundary layer is still in the project, has the same name, and that the data source is valid. If the data source is invalid, a red exclamation mark is placed beside the name of the layer in the table of contents.

Error 14009 Selecting a Field in Spatial Trend Analysis**Description**

"The boundary layer selected is no longer valid. Restart routine to refresh."

Cause

While updating the field values list box, the boundary layer is found to be missing or invalid.

Solution

Ensure that the boundary layer is still in the project, has the same name, and that the data source is valid. If the data source is invalid, a red exclamation mark is placed beside the name of the layer in the table of contents.

Error 14019 Launching ClearAll with F11 from Spatial Trend Analysis**Description**

"Unable to run clear all. There is an installation problem."

Cause

To clean up the project while Spatial Trend Analysis is open, the hot-key F11 can be used. The F11

Attachment A

key launches the Clear All button, available from the OmegaGIS Toolbar in ArcMap. If a problem exists with the [Clear All](#) button, cleaning the project is not possible.

Solution

Contact [The Omega Group](#) to retrieve the appropriate files.

Error 14020 Setting the Layers for Spatial Trend Analysis**Description**

"No incident layers found in the active data frame. Spatial Trend Analysis is unavailable."

Cause

During the setup of the [Spatial Trend Analysis](#) dialog, the table of contents in ArcMap is searched for layers that meet certain criteria for querying. To show up in the Spatial Trend Analysis dialog, a layer must meet this criteria otherwise the layer is not added to the list.

This error is issued if there are no layers on which to base Spatial Trend Analysis.

Solution

Identify the layers that should be used in a Spatial Trend Analysis, ensure they meet the following criteria:

1. The layer has a geometry type of point
2. The layer is a feature layer
3. The layer is not a selection layer. For example, the data source of the layer is not based on another layer in the table of contents.

4. The layer has a valid data source.

5. If 'Use Registered Types' is selected in OmegaGIS Setup, ensure the layer is registered with one of the types selected, or unselect the 'Use Registered Types' option.

6. If 'Exclude layers created by OmegaGIS...' is selected in OmegaGIS Setup, ensure the layer was not created by an OmegaGIS routine, or turn off this option.

Error 14011 Boundary Layer Selection Field in Spatial Trend Analysis

Description

"Selection field does not exist in the boundary layer. Spatial Trend Analysis cannot continue."

Cause

The field used to select polygons from the boundary layer is missing.

Solution

Open the Spatial Trend dialog, and select the boundary layer again. Select a field name from the list provided.

Error 14013 Map Units for Spatial Trend Analysis

Description

"The map units are not set for the active data frame. Spatial Trend Analysis cannot continue."

Cause

Attachment A

The map units are not set on the active data frame in ArcMap. The units are necessary for the Spatial Trend Analysis calculations.

Solution

Right click on the data frame and select properties. Select the General tab, and ensure that the Map Units are set.

15000 to 15050: Layout Metadata Editor

This section contains the error messages for the [Layout Metadata](#) Editor.

Error 15000 Opening Dialog

Description

"The active view must be a 'Data View' rather than the 'Layout View' in order to open OmegaGIS dialog."

Will not enable the tool until this issue has been resolved.

Cause

The active data frame is in layout view rather than data view. The data view shows the data in the map and hides the map layout.

Solution

Switch to active data frame to the layout view by selecting the button with the image of the paper at the bottom right of the active data frame



Error 15032 Setup Settings

Description

"Disclaimer not found in setup database."

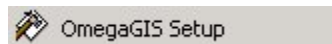
Occurs when the Layout Metadata Editor dialog is opened.

Cause

The setup database has been expanded to accept many more settings than before. This means that new settings are referenced in OmegaGIS tools but might not exist in setup database used in previous products. This error is caused by the setting 'Disclaimer' not existing in the Setup.mdb.

Solution

Open the setup dialog either by opening the Main Menu and clicking the setup button or by opening it up through the tool bar. Once a setup database from a previous version is opened, it is automatically upgraded to the current version.



6701001 to 7800999

6701001 Dialogs in ArcCatalog

Description

"ArcCatalog must be restarted to use OmegaGIS. Ensure that ArcGIS Service Pack 1 is installed."

Occurs when an OmegaGIS dialog is opened in ArcCatalog.

Cause

An error was introduced at ArcGIS 9.0 that prevents non-modal dialogs from opening in ArcCatalog.

Solution

Attachment A

This issue has been resolved with Service Pack 1 for ArcGIS 9.0 that is available from the ESRI support web site. If Service Pack 1 for ArcGIS 9.0 has been installed, then restart ArcCatalog as changes to the registry have been made that require a restart of ArcCatalog to take effect.

7800102 Query and Density Dialog

Description

"The active view must be a 'Data View' rather than the 'Layout View' in order to open OmegaGIS dialog."

Occurs when the Query or Density dialog is opened.

Cause

The active data frame is in *layout view* rather than *data view*. The data view shows the data in the map and hides the map layout.

Solution

Switch to active data frame to the data view by selecting the button with the image of the globe at the bottom right of the active data frame



7800103 Query and Density Dialog

Description

"There are no Feature Layers in the active data frame; unable to open OmegaGIS dialog."

Occurs when the Query or Density dialog is opened.


Cause

This error occurs when there are no valid feature layers in the active data frame. A feature layer is

Attachment A

defined as a layer based on a feature class in a vector geographic dataset such as a geodatabase, ESRI shapefile or ArcInfo coverage.

A layer is not valid when the data source of the layer is missing. When the data source is missing the layer has a red exclamation mark in the table of contents.

 2002 Part I Crimes

Solution

- Change the active data frame to one that contains feature layers.
- Add feature layers to the active data frame.
- Fix the issue that caused the missing data source.

7800211 Near a Feature Routine

Description

"The feature layer to be used with routine is no longer in the active data frame."

Occurs when a layer is selected from the list of feature layers on the **Where?** tab for the Near a Feature routine.

Cause

The selected layer in the list of feature layers on the Where? tab for the [Near a Feature](#) routine has been removed from the active data frame.

Solution

Close the query dialog and then add the layer back to the active data frame. Then open the query dialog again.

Attachment A

780221 Near An Address Routine

Description

"The address was not geocoded."

This warning occurs when the Check Address button is selected while running the [Near An Address](#) routine.

Cause

The address entered could not be geocoded.

Solution

- Ensure that the address is spelled correctly.
- Alter the geocoding properties by reducing the spelling sensitivity or minimum match score.

7899226 Hot Spot Routine

Description

"Unable to use the Hot Spot routine; the Spatial Analyst extension must be enabled."

Occurs when the [Hot Spot](#) button is selected on the Density Map dialog.

Cause

The Spatial Analyst extension is not enabled. Information on which extensions are enabled is based on the current user logged into the machine, and is stored in the computers registry (HKEY_CURRENT_USER). When an extension is enabled all new or existing ArcMap documents have that extension enabled. If a different user logs into the machine, the Spatial Analyst extension must be enabled.

Attachment A**Solution**

Enable the Spatial Analyst extension. To enable the extension, Spatial Analyst must have been installed and it must be licensed appropriately from ESRI. There are two ways to enable the Spatial Analyst extension:

- From the Tools pull-down menu in ArcMap, select Extensions. Check the Spatial Analyst extension. If Spatial Analyst is not available in the list of extensions, then it has not been installed. If the Spatial Analyst extension is not licensed there is a message box issued when the extension is selected.
- To automatically enable the extension, check the "All extensions used with OmegaGIS routines will be automatically enabled..." option in the [OmegaGIS Setup](#) dialog.

7800400 Date Range Validation

Description

"Invalid date range selected. FROM date (*) is greater then the TO date (*)."

This validation error occurs when the Finish button is selected and all of the parameters of either a query or density map routine have been entered.

Cause

The FROM date (the beginning of the date range) that has been selected occurs after the To date (end of the date range).

Solution

Change the [date range](#) selected ensuring the beginning of the date range is before the end date.

7800401 Boundary Layer Validation

Attachment A**Description**

"No features selected in the boundary layer (*)."

This validation error occurs when the Finish button is selected for the [Incidents Within A Boundary](#), [Hot Spots](#) or [Repeat Calls](#) routine.

Cause

When the "By Pointing" selection method is used to identify features in the boundary layer, the routine checks to ensure that there are selected features in the boundary layer. This error occurs when no features have been selected in the boundary layer.

Solution

- Select features in the boundary layer using the ["By Pointing"](#) selection method.
- Use the ["By Field Value"](#) method to select features in the boundary layer.

Tip:

One way to determine how many features are selected in a layer is to use the Omega tab.

7800402 Date Range Validation**Description**

"The query layer (*) has no information for at least one of the dates selected (* to *)."

This warning occurs when the Finish button is selected for Queries and Density Maps routines. There is an option with this warning to continue to run the routine.

Cause

The FROM and TO calendars have the option to display the query layer's available [date range](#). When the date range is displayed and either the beginning date or the end date selected is not within the query

Attachment A

layer's available date range this warning occurs.

Solution

Either select "Yes" and continue to run the routine with the selected date query or "No" and alter the date query.

7800413 Feature Layer Validation

Description

"No items have been selected in the feature layer (*)."

This validation error occurs when the Finish button is selected for the [Near A Feature](#) routine.

Cause

When the "By Pointing" selection method is used for selecting features in the feature layer, the routine checks to ensure that there are selected features. The error occurs when no features have been selected in the feature layer.

Solution

- Select features in the feature layer using the ["By Pointing"](#) selection method.
- Use the ["By Field Value"](#) method to select features in the boundary layer.

Tip:

One way to determine how many features are selected in a layer is to use the Omega tab.

7800420 User Defined Area

Attachment A**Description**

"Invalid user-defined area; only one polygon graphic element can be selected in the active data frame, currently there are *."

This validation error occurs when the Finish button is selected for the [Within A Boundary](#), [Density Map](#), [Hot Spot](#) and [Repeat Calls](#) routine; and a user defined area is used to identify the spatial query.

Cause

Only one graphic element may be selected when using a [user defined area](#). An element is selected when it has handles around it's envelope.

Solution

- Select only one graphic element by using the Select tool in ArcMap. Make the Select tool active and then select the graphic element to be used with the routine.
- Remove all of the graphic elements using the Clear All routine and then create a new user-defined area.

7800423 User Defined Area

Description

"Invalid user-defined area; the selected graphic element is a union of multiple polygons which is not supported."

This validation error occurs when the Finish button is selected for the [Within A Boundary](#), [Density Map](#), [Hot Spot](#) and [Repeat Calls](#) routine; and a user defined area is used to identify the spatial query.

Cause

The selected graphic element that is to be used as the user defined area has more than 1 exterior ring.

Solution

Attachment A

Remove all of the graphic elements using the Clear All routine and then create a new user-defined area.

7810000 to 7810500

7810120 Query Layers

Description

"Unable to find query layer(s): *"

This error occurs during the running of a Query or Density Map routine.

Cause

One or more [query layers](#) could not be found in the data frame. The layer has either been renamed, removed or is not valid.

Another potential cause is that the layer name has trailing spaces. These trailing spaces are the source of the problem as the routine is searching for the layer by it's name without the trailing spaces.

Solution

- Close the Query or Density dialog and open it again. This will ensure that the list of query layers is updated based on the layers in the active data frame. With the list of query layers updated, select the appropriate layers and run the routine again.
- Remove any trailing spaces from the layer name.

7810124 Boundary Layer

Description

"The boundary layer '*' is not valid; check the data source of the layer."

This error occurs during the running of a Query or Density Map routine.

Cause

The boundary layer data source has been moved, renamed, deleted or is currently unavailable. When the data source is missing the layer will have a red exclamation mark in the table of contents.

Solution

- Determine the problem with the data source of the boundary layer and make the necessary correction. One solution would be to remap the data source, this is done by selecting the Set Data Source button on the "Source" tab on the Layer Properties dialog.
- Use a different boundary layer.

7810126 Boundary Layer

Description

"The boundary layer '*' could not be found in the data frame (*)."

This error occurs during the running of a Query or Density Map routine.

Cause

The boundary layer could not be found in the data frame, the layer has either been removed or renamed.

Solution

Attachment A

Close the dialog and then open it again; the list layers to use for a boundary layer will be updated.
Select a boundary layer.

781028 Feature Layer

Description

"The feature layer '*' is not valid; check the data source of the layer."

This error occurs when running the [Near A Feature](#) routine.

Cause

The feature layer data source has been moved, renamed, deleted or is currently unavailable. When the data source is missing the layer will have a red exclamation mark in the table of contents.

Solution

- Determine the problem with the data source of the feature layer and make the necessary correction. One solution would be to remap the data source, this is done by selecting the Set Data Source button on the "Source" tab on the Layer Properties dialog.
- Use a different feature layer.

7810138 Near An Address

Description

"The geocoding service '*', cannot be found in the ArcMap document."

This error occurs when running the [Near An Address](#) routine.

Cause

Attachment A

A geocoding service is required to run the Near An Address routine. The error occurs when the geocoding service is no longer referenced by the ArcMap document.

Solution

Add a reference to a geocoding service with the Geocoding Services Manager dialog. This can be opened from the Tools -> Geocoding pull-down menu in ArcMap or by selecting the Add/Remove button on the Where? tab for the Near An Address routine.

7810305 SQL Query

Description

"SQL syntax error when querying the layer '*' (*)."

The error occurs when running a Query or Density routine that uses [additional query layers](#).

Cause

The error occurs when selecting the incidents in an additional query layer with a SQL attribute query. The problem is with the syntax of the SQL query.

Solution

Check the syntax of the SQL query. ArcMap's Select By Attribute dialog is useful in determining the correct SQL syntax. If necessary, update the Saved Query with the OmegaGIS Saved Query Editor.

7810306 Additional Query Layers

Description

"No features have been selected. Unable to complete the routine."

This error occurs when running a Query or Density routine that uses [additional query layers](#).

Attachment A**Cause**

No features in the query layer and the additional query layer(s) satisfied the attribute and or spatial query.

Solution

Use a different attribute or spatial query and then run the routine again.

7810307 SQL Query

Description

"SQL syntax error when querying the layer '*' (*)."

This error occurs when running a Query or Density routine that does not use additional query layers.

Cause

The error occurs when selecting incidents in the query layer with a SQL attribute query. The problem is with the syntax of the SQL query.

Solution

Check the syntax of the SQL query. ArcMap's Select By Attribute dialog is useful in determining the correct SQL syntax. If necessary, update the Saved Query with the OmegaGIS Saved Query Editor.

7810308 Query Layer

Description

"No features have been selected. Unable to complete the routine."

This error occurs when running a Query or Density routine that does not use additional query layers.

Attachment A**Cause**

No features in the query layer satisfied the attribute and or spatial query.

Solution

Use a different attribute or spatial query and then run the routine again.

7810415 Near An Address

Description

"Unable to geocode the address [*]."

The error occurs when running the Near An Address routine.

Cause

The address provided cannot be geocoded, consequently the Near An Address routine cannot be completed.

Solution

- Ensure that the address is spelled correctly.
- Alter the geocoding properties by reducing the spelling sensitivity or minimum match score.
- Use the "Check Address" button on the Where? tab to determine if the address can be geocoded before running the routine.

1100101 to 1100150: OmegaGIS Setup

This section contains the error messages for the [OmegaGIS Setup](#) dialog.

Error 1100102 Opening Dialog

Description

"This user does not have permissions to write to the Setup database."

Error can occur when dialog is loading.

Cause

The Setup.mdb located in the project workspace lacks write permissions.

Solution

Open Windows Explorer and navigate to the project directory. Right-click the file Setup.mdb and select 'Properties' from the menu. If the 'Read Only' box is checked then click it off.

Warning 1100105 Processing Request

Description

"To use registered layers to make new queries, at least one registered type must be selected."

Error can occur when 'OK' or 'Apply' is clicked.

Cause

This warning occurs when in the 'Queries' Category on the 'Registered Types' tab the check box is checked but no vales in the list are checked.

Solution

Check the registered types in the list that will be used as query layers.

Warning 1100106 Processing Request**Description**

"Some Threshold Alert recipient Email addresses reference the default SMTP server. There is no default SMTP server set."

Error can occur when 'OK' or 'Apply' is clicked.

Cause

This warning occurs when in the 'Threshold Alert' Category emails are specified but no default server is specified. Each email must be associated with an SMTP Server. If there are no servers set then the emails are added to the default server. If no default server is set when 'OK' or 'Apply' is clicked then this warning will result.

Solution

On the 'SMTP Server' tab of the 'Threshold Alert' Category set one of the servers in the list as the default. This is done by selecting the server clicking the 'Edit' button and checking the 'Use this server as the default' box.

4100100 to 4100300: Threshold Alert

This section outlines the error messages for [Threshold Alert](#).

4100112 Accessing the Threshold Alert Database**Description**

"Release_Info table was not found."

Cause

Attachment A

When threshold alerts are run, the project folder is searched for the threshold_alert.mdb database. Within the database is a table called Release_Info that provides the major and minor release codes of the database. This information is important to determine whether the database is up to date with the release of the OmegaGIS software.

This error occurs because while searching for this information in the threshold_alert.mdb database, the table was not found.

Solution

Contact your project manager to either upgrade the database or modify the existing structure to work with OmegaGIS Threshold Alerts.

4100113 Accessing the Threshold Alert Database**Description**

"Database is out of date."

Cause

When threshold alerts are run, the project folder is searched for the threshold_alert.mdb database. Within the database is a table called Release_Info that provides the major and minor release codes of the database. This information is important to determine whether the database is up to date with the release of the OmegaGIS software.

If the major and minor release codes are not current to the release of the OmegaGIS software, this message is issued.

Solution

Contact your project manager to upgrade the database.

4100101 Accessing the Threshold Alert Database

Description

"Database file has not been set."

Cause

While the path to the Threshold_Alert.MDB database was being set, the path was lost.

Solution

The processing of the threshold alert was interrupted, and the database path was not completed. Run the threshold alert again to update the database path.

4100102 Accessing the Threshold Alert Database**Description**

"Database file was not found."

Cause

The threshold_alert.mdb database should be located in the root folder of the [project](#). On searching for the database in this folder, the database was not found.

Solution

Find the threshold_alert.mdb database using Windows Explorer, and move the database to the project folder if required. Ensure the database is called threshold_alert.mdb.

4100103 Running Threshold Alert Automatically**Description**

"Database password has not been set."

Attachment A**Cause**

The program was interrupted when collecting the password information for the threshold_alert.mdb database.

Solution

The processing of the threshold alert was interrupted, and the database password was not set. Run the threshold alert again to update the password.

4100104 Running Threshold Alert Automatically**Description**

"Database password is incorrect."

Cause

The password used to open the threshold_alert.mdb database is incorrect.

Solution

Contact your project manager, to ensure that the correct version of the threshold_alert.mdb database is in use.

4100202 Running Threshold Alert Automatically**Description**

"Database password is incorrect."

Cause

The password used to open the threshold_alert.mdb database is incorrect.

Solution

Contact your project manager, to ensure that the correct version of the threshold_alert.mdb database is in use.

4100600 to 4100700: Cyclical Reports

This section contains error numbers for [Cyclical Reports](#).

4100610 Updating the Save Cyclical Dialog

Description

"Project XML file cannot be found."

Cause

The project XML file is not in the project workspace.

Solution

Run an OmegaGIS Query, Density or Analysis routine to recreate the project XML file.

4100611 Accessing the Setup Database

Description

"Error connecting to Setup database."

Cause

Attachment A

An ADO connection is used to connect to the Setup.mdb in the project workspace. This error occurs when the connection fails.

Solution

The Setup.mdb database may be corrupt, or the table itself may be corrupt. Delete the setup database from the project workspace. It is recreated the next time OmegaGIS is run.

4100612 Accessing the Setup Database**Description**

"Error connecting to table Omega_SetupLoc in setup database."

Cause

The Setup.mdb database contains a table called Omega_SetupLoc that identifies the paths that should be searched for report templates, when a report is run. If a problem occurs while trying to access this table, this error is issued.

Solution

The Setup.mdb database may be corrupt, or the table itself may be corrupt. Delete the setup database from the project workspace. It is recreated the next time OmegaGIS is run.

4100637 Running a Cyclical Report**Description**

"Unable to run Cyclical Report; the Clear All routine is not installed correctly."

Cause

The Clear All routine is used to refresh the layers in ArcMap after a Cyclical Report is run. If this routine is not installed correctly, has become corrupt or is missing, this error is issued.

Solution

Reinstall OmegaGIS to refresh the Clear All routine.

4100638 Running a Threshold Alert**Description**

"Unable to run Threshold Alert; the Clear All routine is not installed correctly."

Cause

The Clear All routine is used to refresh the layers in ArcMap after a Threshold Alert is run. If this routine is not installed correctly, has become corrupt or is missing, this error is issued.

Solution

Reinstall OmegaGIS to refresh the Clear All routine.

470000 to 470100: OmegaGIS Field Manager

This section contains the error messages for the OmegaGIS [Field Manager](#).

Error 470002 Duplicate Field Name**Description**

"The field name is already contained in the dataset."

Before the Field Manager creates and adds the new field to the dataset, the dataset is searched for the field name entered in order to prevent duplicate field names.

Cause

The field name entered was found in the dataset. The field cannot be created.

Solution

Enter a new field name that is not already contained in the dataset.

Error 470001 Source Field Not Found**Description**

"A source field no long exists in the feature class. It may have been removed or updated. Close the utility and reopen to refresh the list of source fields."

The routine is validating whether the source field identified for creating either a Date or Time OmegaGIS field is in the selected feature class.

Cause

The source field to be used to create the new OmegaGIS Date or Time field could not be found in the selected feature class.

Solution

Close the OmegaGIS Fields Manager, and reopen. Closing the utility refreshes the list of available source fields.

Error 470002 Duplicate Day of Week Field**Description**

"The name selected for the new Day of Week field already exists in the feature class. Enter a new name to continue."

The routine is validating whether the Day of Week field name selected already exists in the select

Attachment A

feature class.

Cause

The Day of Week field name entered on the form already exists in the feature class. Duplicate field names cannot be added to the same feature class.

Solution

Enter a different name into the Day of Week field name text box on the form.

Error 470003 Duplicate Field Name in Metadata**Description**

"A duplicate field name was found in the metadata. Open the OmegaGIS Metadata Editor on the selected layer, and click the 'OK' button in order to remove duplicate metadata."

The field manager is reading the metadata of the selected layer. A duplicate field name was found in the metadata. Layers cannot contain duplicate field names.

Cause

While the Field Manager was reading the names of the fields in the metadata, a duplicate field name was encountered. The Remove and Update field lists cannot contain duplicate field names. The Field Manager will not load with duplicate field names in the metadata. has been registered as versioned. The Omega Import Wizard only supports the updating of non-versioned feature classes.

Solution

Use the OmegaGIS Metadata Editor in order to clean up the metadata of the layer. The Metadata Editor will remove duplicate field names generated in the layer's metadata. Open the Metadata Layer with the layer in question, and click the OK button to clean the metadata.

Error 470004 Missing Information

Description

"Unable to perform the test due to missing information. Ensure that the sample and format text boxes contain information."

The Test button was clicked in order to test whether the selected format matches the source information.

Cause

The Sample text box and the Format text box information are both required in order to perform the test. At least one of these text boxes on the dialog is missing information.

Solution

Ensure that both the Sample text box and the Format text box contain information that can be used to test whether the source data matches the format selected.

Error 470007 OmegaGIS Reserved Field Names

Description

"The new field name is an OmegaGIS reserved field name. Select a new name to continue."

The new field name selected by the user is a reserved field name used by OmegaGIS routines.

Cause

Before the OmegaGIS Fields Manager creates a new field, the field name is checked to ensure that it is not a reserved field name created by other OmegaGIS routines. The field name entered is found to be one of these names.

Solution

Attachment A

Enter a new field name that is not an OmegaGIS reserved field name.

Error 470009 Invalid Characters**Description**

"The new field name contains an invalid character."

The new field name entered contains an invalid character, for example an apostrophe or pound sign.

Cause

Field names cannot include certain characters. A character that cannot be used with the dataset selected has been found in the new field name.

Solution

Create a new field name that does not include special characters.

Error 470010 Field Name Length**Description**

"The new field name is too long."

Depending on the data type of the dataset, fields may have a length limitation. In this case, the field name entered has exceeded the allowable length.

Cause

The field name entered has exceeded the allowable field length for the dataset. The allowable field length may change according to the type of dataset selected.

Solution

Create a new field name that does not contain as many characters.

Error 470011 SQL Reserved Words**Description**

"The new field name is a SQL reserved word."

The field name is a SQL reserved word. Standard SQL reserved words include 'SELECT', 'UPDATE', 'DATE' and 'TIME'. Other words may also be included in this list, but are dependent on the format of the dataset.

Cause

The new field name is a SQL reserved word and cannot be created in the dataset.

Solution

Create a new field name that is not a SQL reserved word. Read the ArcGIS documentation for an explanation of SQL reserved words.

8010000 to 8020999: Omega Street Network

This section contains the error messages for the [Omega Street Network](#). The Omega Street Network is used to provide networking functionality and this is used by the FireView routines.

8020566 Summarize Running Order

Description

"Unable to summarize the running order. Ensure appropriate version of the JET engine is installed (Windows 2000, Service Pack 4 required). [*]"

Attachment A

Occurs when a Cost Matrix is being generated.

Cause

The RunOrder field in the CostMatrix_* feature class is summarized and the results are placed in the RunOrder_Lookup_* table. The SQL functionality used to summarize the RunOrder field is the cause of the problem. The RunOrder field in the CostMatrix_* feature class has the Memo field type and there is an issue with the Microsoft Jet 4.0 engine and Memo fields. Refer to Microsoft Knowledge Base Article 304431 for more information.

Solution

- Install the latest Microsoft Jet 4.0 service pack.
- When the computer is running Windows 2000, install Windows 2000 Service Pack 4 as this contains a Microsoft Jet 4.0 service pack that will resolve the issue.

CrimeView Analytics

Better Insight, Smarter Policing



WHAT IS THE PROBLEM

Law enforcement practices are under more scrutiny than ever before. Agencies need information and data that helps them deploy smart policing based on informed, data-driven decisions. There is a lot of data out there. But a lot of data doesn't necessarily translate into better decisions and protocols, and in fact can just be added noise that can lead to wasted time and effort.

WHAT ARE THE BENEFITS

CrimeView Analytics combines disparate data sources for easy analysis that empowers your agency to operate efficiently and effectively. With timely insight into trends, patterns and behavior, agencies can proactively respond to situations that promote officer and citizen safety. Utilizing Esri mapping technologies, CrimeView Analytics allows users to create powerful and easy-to-understand dashboards and reports to share with others. Delivered as a single solution from the AWS GovCloud, CrimeView Analytics provides agencies with configurable, easily accessible and visually relevant displays of measurable and achievable goals.

SMARTER PATROL, SMARTER POLICING

Bring analytics and mapping into your patrol work with actionable information for your agency's proactive policing strategies. Integrate with your Mobile system and use the Esri-based maps and components drill down to specific geo data, like districts. Simplify administration time by automatically generating and delivering role-based reports and dashboards to supervisors and authorities. Create briefing books that can restrict viewable data based on role, organizational unit, geography or crime priority. Enable threshold alerting to receive automatic live alerts as irregular activities occur.

WHAT IS THE SOLUTION

Make your data work the way you need it to. Whether it is an alert to a situation that needs immediate attention, or an evaluation over a time period for process improvements, you'll be better equipped with CrimeView Analytics.

FEATURES

- Analysis and Dashboard Modes
- Esri Maps with User Data (i.e. districts, beats, etc.)
- On-Demand Queries
- Scheduled Report Generation
- Threshold Alerting
- Address Geo-verification
- Density Maps
- User Based Security



SECURE, PERMISSION-BASED ACCESS

Deployed in AWS GovCloud, your data is protected with world class security encryption that is CJIS, ITAR, and FIPS compliant. CentralSquare’s proven identity management ensures complete CJIS compliance and user management, which Administrators can easily configure for existing and new users.

DATA SETS

- Incidents
- Warrants
- Record
- Field Interviews
- Citations
- Arrest
- Accident

ANALYSES

- **Intelligence Analysis** – use Analysis mode to link incidents and records based on geographical area, person(s), etc.
- **Criminal Investigative Analysis** – use Analysis mode to visually represent criminal incidents, trends and serial patterns to assist in criminal investigations.
- **Tactical Analysis** – use Dashboard mode to show where, when and what crimes occurred to predict resource requirements and track progress.
- **Strategic Analysis** – improve strategic planning and budget allocation with macro analysis to deploy resources effectively.
- **Administrative Analysis** – create and present dynamic dashboards to visually show incident data/trends for internal, city and state leaders.
- **Operational Analysis** – analyze your department’s response times, call times, average units dispatched and other key operational metrics by location, call type, officer, etc.

WHO WE ARE

CentralSquare Technologies is an industry leader in public safety and public administration software, serving over 7,650 organizations from the largest metropolitan city to counties and towns of every size across North America.

CentralSquare’s broad, unified and agile software suite serves 3 in 4 citizens across North America. Our technology platform provides solutions for public safety, including 911, computer aided dispatch and records management. For public administration agencies, CentralSquare provides software for finance, human capital management, payroll, utility billing, asset management and community development.

More information is available at www.centalsquare.com.

BRING DIVERSE DATA SETS INTO A COMMON VIEW

CrimeView Analytics aggregates data from disparate systems and displays it as one seamless experience. In one view, see summaries and correlations from your calls for service, incidents, arrests, field interviews, and much more.

7,650

AGENCY CUSTOMERS

3 in 4

CITIZENS SERVED ACROSS NORTH AMERICA

2000+

EMPLOYEES FOCUSED ON SERVING THE PUBLIC SECTOR

Cybersecurity Program Overview

The CentralSquare Cybersecurity Program implements a series of comprehensive physical and logical controls that align with the NIST Cyber Security Framework and standards to provide a secure, layered defense for all hosted information. CentralSquare maintains annual Payment Card Industry (PCI) and Statement on Standards for Attestation Engagements (SSAE18) compliance through a series of ongoing assessments and security testing performed by a PCI Qualified Security Assessor and AICPA auditor. Adherence to these standards ensures all controls are met specific to access, transmission, processing, and storage of data.

- **Secure Software Development**
- **Vulnerability Management**
- **Incident Response**
- **Business Continuity Management**
- **Government Cloud**
- **Regulatory Compliance**





Secure Software Development

CentralSquare implements secure coding best practices throughout the development lifecycle. Where supported, CentralSquare-developed applications undergo rigorous automated and manual testing and analysis. The lifecycle approach ensures that security is embedded into every application we develop.

Secure Software Lifecycle Management:

- **Requirements & Design**
 - Annual OWASP-based Developer training
 - Application Readiness Assessments to identify security gaps
- **Software Construction/Development**
 - Developer IDE Code Analysis
 - Real-time feedback on coding best practices & potential security flaws
- **Deployment & Maintenance**
 - Weekly Security “Scrum” with key stakeholders to address open security flaws
 - Monthly review with Product Directors to address application security strategy & timelines

Static Application Code Analysis

- **Service:** Third Party Independent Service
- **Methodology**
 - Binary code scan, executed during software construction stage of SDLC
 - Performed in a non-runtime environment; evaluates both web and non-web applications
 - Inspect compiled versions for flaws, malicious code, back doors etc.
 - Risk-based approach to remediation

Dynamic Web Application Scanning

- **Service:** Third Party Independent Service & Internal Scan Utility
- **Methodology**
 - Phase 1: Spider phase. Enumerate exposed functionality & attack surface
 - Phase 2: Attack & detect exploitable vulnerabilities as the application operates
 - Baseline derived from SANS Top 25 & OWASP Top 10 vulnerabilities
 - Risk-based approach to remediation

Advanced Application Security Assessments

- **Service:** Third Party Independent Service
- **Methodology**
 - Penetration testing of web-based applications, executed testing/validation stage of SDLC
 - Phase 1: Active & passive discovery including vulnerability scan
 - Phase 2: Manual, authenticated assessment to identify logic flaws, privilege escalation etc.
 - Remediation required for all confirmed findings. Timeline dependent on severity + overall risk



Vulnerability Management

Scanning and Remediation

The CentralSquare Scanning and Remediation Program is a critical component of secure software development & maintenance. Through a holistic approach to vulnerability management, CentralSquare identifies and correlates application, network and system issues to ensure effective, timely remediation and resolution.

External Perimeter Scanning

- Frequency: Weekly, or Ad Hoc upon request
- Methodology
 - Detect & classify network and system vulnerabilities for all owned/leased/hosted IP ranges
 - Remediation or Risk Acceptance required for all confirmed issues
 - Remediation timeline dependent on severity + overall risk to the Business Unit

Payment Card Industry Vulnerability Scanning & Penetration Testing

- Service: Third Party Independent Service
- Frequency: Quarterly (Vulnerability Scan) & Annual (Penetration Test)
- Methodology
 - Detect & exploit vulnerabilities as per PCI scanning requirements
 - Segmentation testing to ensure logical separation of Card Data Environment
 - Remediation required for external issues w/CVSS score of 4.0 or higher, to maintain PCI compliance
 - Remediation required for internal issues identified as High or Critical, to maintain PCI compliance

Advanced Network Security Assessments

- Service: Third Party Independent Service, performed by Depth Security
- Frequency: Annual
- Methodology
 - Phase 1: Information Gathering, define attack surface
 - Phase 2: Cross-reference open services with known vulnerabilities
 - Phase 3: Penetration test of network perimeter
 - Phase 4: Attempt to compromise target systems

Application & Scanning Vulnerability Remediation Process

- Confirmed Critical vulnerabilities are driven to a 30 day remediation timeline
- Confirmed High vulnerabilities are driven to a 60 day remediation timeline
- Vulnerabilities are driven to remediation or risk acceptance, per prescribed timelines
- Open vulnerabilities are reported weekly, with remediation plans updated bi-weekly



Incident Response

The Security Incident Response Policy establishes the steps needed to properly handle information security incidents, both suspected and actual, at CentralSquare. Incidents can include any event that could disrupt the confidentiality, integrity, or availability of CentralSquare systems and/or company and customer information. Procedures for detecting and responding to incidents are in place and employees are aware of the appropriate escalation steps.

DETECTION

Signs of a security incident may be obvious or subtle. Electronic security incidents may not immediately appear to affect sensitive systems or information, but could occur in a supporting system that directly or indirectly allows access to this information. Thus, any unusual activity or irregularity to configuration of systems or applications can signify a breach. CentralSquare has multiple tools in place to alert on an incident, including but not limited to: Security Information & Event Managers (SIEM), Syslog, Intrusion Prevention Systems (IPS), Web Filtering Services, Web Application Firewalls, and Advanced Threat Protect Engines.

RESPONSE

- Assess the nature of the incident. Invoke the CentralSquare Playbook for Managing a Data Breach, if necessary.
- Determine if CentralSquare staff or customers are affected by the incident. If customers are affected, an immediate plan will be developed to mitigate the problem and notify affected individuals. If customers are impacted the CentralSquare legal team will be notified.
- Determine potential signs of fraud. If fraud is suspected, the Human Resources and Legal departments will be notified.
- CentralSquare will notify impacted staff and customers within two business days (48 hours) of a confirmed incident.

REPORTING

In the event of a confirmed security incident, a detailed report is written that includes;

- Affected staff, customers, data, computing systems, and other property
- Response steps
- Root cause analysis

TESTING

The incident response plan will be tested annually via one of the following methods, unless already invoked during the current year for a suspected or actual incident:

- Table top exercise. Each employee will simulate their response based on the scenario given.
- Simulated incident. Notify appropriate management staff in advance and schedule a date to begin test. Establish protocols that will distinguish the test from a real security incident.

REVISION

The incident response plan will be refreshed on an as-needed basis, not to exceed 12 consecutive months.

- After a confirmed incident, a lessons learned analysis will be performed with relevant policy revisions.



- All plan revisions are reviewed and approved by management.

Business Continuity Management

The Business Continuity Management program (BCM Program) is a process designed to oversee the CentralSquare's ability to provide adequate business and technology recovery plans, capabilities to manage recovery of operations, identification of resiliency risks and rapid response during a disaster recovery crisis event.

All CentralSquare business functions develops, maintains and continually improves business continuity and disaster recovery plans. The purpose of these Plans are to:

- Protect life, information and assets of CentralSquare, respectively.
- Conform to applicable regulatory, insurance and ethical business practices.
- Support and be in agreement with the CentralSquare's tactical and strategic business plans.
- Minimize the impact of Disaster on our clients, employees and the business associates to whom services are provided.

CentralSquare has a comprehensive BCM Program in place including.

- Business Impact Analysis (BIA).
- Business Continuity Plan (BCP)
- Defined SLAs (Service Level Agreement), RTOs (Recovery Time Objective) and RPOs (Recovery Point Objective).
- Annual Disaster Recovery tests and/or Tabletop exercises, to include validation of recovered environment.
- Training and Annual Review



Government Cloud Solutions

The CentralSquare Cloud Security Program ensures 24x7 availability, integrity, and protection of customer information by leveraging a multi-faceted, layered approach to data security.

Physical & Environmental

Recorded Internal and External CCTV
Proximity Card Access Control to Facility; Dual Factor in Secure Areas
Intruder and Door Alarms
Best of Breed HVAC, Fire Suppression, and Physical Security

Monitoring & Availability

24x365 Staffed Operations Facility
24x365 Automated Network Monitoring, Incident Creation and Escalation
24x365 Distributed Denial of Service Mitigation
24x365 Intrusion Detection and Prevention Systems

Vulnerability Management

3rd Party and Internal Perimeter Vulnerability Scanning
Formal Application Security Scanning Program
Annual 3rd Party Penetration Testing
Centrally Managed Endpoint Protection on all Servers
Centrally Managed Patching and Operating System Hardening Program

Logical Access

VLAN Data Segregation
Extensive Deny-By-Default Access Control Lists
Multi-Factor Authentication for System Administration

Business Continuity

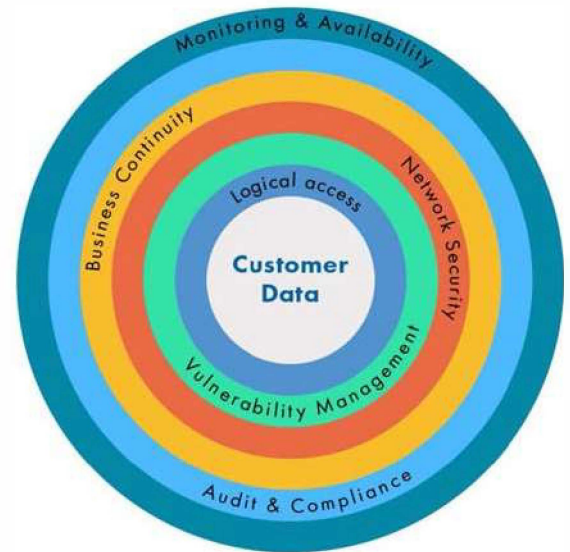
Daily Encrypted Backups stored offsite
Virtual Tape Backup Technology eliminates threat of lost physical media
Replication to Disaster Recovery Location
Internet Redundancy and High Availability using Multiple Carriers

Audit Compliance

Annual SSAE16/ISAE 3402 Data Center Audit
Annual SSAE16 Operations Audit
Annual Control Self-Assessment
Annual PCI-DSS Compliance Audit
Defined Information Security Program and Policy Framework

Network Security

SSL and IPSEC VPN with 256 Bit Encryption
Data-At-Rest Secured with 256 Bit AES Encryption where available
Web Application Firewall Protection
Multi-layer Infrastructure Security Model





Regulatory Compliance

As a provider of public administration and public safety software to government organizations, CentralSquare is subject to a comprehensive set of regulatory and customer audit obligations. These requirements drive the security and compliance framework that governs the CentralSquare business strategy and its employees, products, processes, and technology.

Maintaining customer data security requirements and industry regulatory compliance helps enable CentralSquare to be a market leader, as well as a trusted partner for the customers we serve. Most importantly, it helps to ensure the safety of sensitive citizen information.

PCI DSS: Payment Card Industry Data Security Standard. CentralSquare is a Level 1 provider of credit card processing which means we store, process, and transmit over 6 million one-time and/or recurring credit card transactions per year on behalf of the citizens we serve. Level 1 compliance carries the most stringent requirements as directed by the PCI DSS standard. These requirements are becoming increasingly complex and challenging every year, as bad actors discover new and easier ways to exploit systems that process, store, or transmit credit card data.

Compliance requirements include but are not limited to the following: annual onsite audit at the CentralSquare Center of Excellence in Lake Mary, recurring internal and external system vulnerability scanning, and application penetration testing. If your role in CentralSquare is to perform duties such as customer support, Cloud administration, application development, or professional services, it is imperative that you understand the proper operating requirements when supporting the CentralSquare Cloud and associated Credit Card Data Environment. The methods in which you access, support, and administer systems in the CentralSquare Cloud must adhere to the requirements set forth by the PCI Council and the CentralSquare Security & Compliance Program.

Maintaining PCI compliance not only means that CentralSquare is adhering to the requirements of the PCI Council, but most importantly it means that we are providing a safe and secure operating environment for the citizens we serve every day.

SSAE18: Standards of Statements on Attestation Engagements, #18. The SSAE18 Audit Standard is governed by the American Institute of Certified Public Accountants [AICPA], and focuses specifically on Data Center Controls relevant to the Hosting of Customer Financial Records. These controls consist of people, processes, and technology implemented to protect customer financial data. Examples include change management for customer production systems and financial applications, physical and environmental data center systems, backup and disaster recovery planning, and proper authentication and authorization into hosted customer environments.

CentralSquare Cloud stores, processes, transmits, and hosts customer financial information and is therefore audited on an annual basis, per the SSAE18 Standard. The audit outcome, along with a formal Auditor Opinion, is detailed in the System and Organizational Controls Report, or SOC Report.



Customers often require the CentralSquare SOC report as part of their annual internal financial audit. The SOC Report is considered sensitive in nature, and should only be provided to active CentralSquare Cloud customers. A redacted version of the report is available for premise customers that process credit card data through the CentralSquare Cloud Hub environment, and a high-level attestation letter can be provided for prospective customers or for purposes of Request For Proposal (RFP).

Ensuring proper protections exist in CentralSquare hosted data centers proactively helps to enable a secure operating environment and successful overall customer experience.

CJIS: Criminal Justice Information Services. Governed by the Federal Bureau of Investigation, the CJIS regulation pertains to proper access, handling, transmitting, processing and storing of Criminal Justice Information, or CJ. Criminal Justice Agencies must comply with all aspects of the CJIS policy, which also extends to non-Criminal Justice Agencies such as CentralSquare.

CentralSquare has an obligation to comply with CJIS specifically for the development, installation, and support of Public Safety solutions that we provide to Criminal Justice Agencies for the purpose of interfacing with FBI CJIS systems that may contain CJ. These applications include CAD, RMS, MCT, OSMCT, Freedom, StateConnect, and Message Switch.

CJIS requirements also extend to the Support system in use by CentralSquare when accessing public safety environments. Currently, Securelink is the approved CJIS Customer Support system due to enhanced features such as multi-factor authentication and FIPS (Federal Information Processing Standard) 140-2 compliance.

CJIS requirements also extend to CentralSquare personnel. To be cleared for support access to customer environments that may contain CJ, employees must complete annual training with a test component, get fingerprinted, and be willing to undergo a background check should the customer require one.

CentralSquare is subject to CJIS audit at both the state and federal levels, as part of overall compliance for our public safety customers. Ultimately, the customer is responsible for ensuring vendor compliance with CJIS, which means the customer can engage CentralSquare for compliance assurances during any CJIS audit engagement.

HIPAA: Health Insurance Portability & Accountability Act. CentralSquare provides public safety software solutions to many customers that fall within the purview of HIPAA; therefore we must meet the Administrative, Technical, and Physical control specifications specific to the safeguarding of Protected Health Information, or PHI.

Specifically, CentralSquare is subject to the requirements of a Business Associate (BA) to a Covered Entity. A Covered Entity is defined as any provider (City, County, University, etc.) that processes, transmits, or stores Protected Health Information.

As a Business Associate, CentralSquare is bound by a Business Associate Agreement for each Covered Entity. Business Associate Agreements set forth requirements to ensure the protection and prevent the disclosure of health information, and set specific provisions for breach reporting as they relate to the exposure of PHI.

FERPA: Family Educational Rights and Privacy Act & PPRA: Protection of Pupil Rights Amendment. FERPA and PPRA are Federal laws intended to protect the rights of students and their families, and the privacy of student education records. The law applies to all institutions that receive funds through the U.S. Department of Education.



CentralSquare is a solution provider to many educational institutions, and therefore must abide by the laws of FERPA & PPRA in regards to proper handling of student data.

GDPR: European General Data Protection Regulation. EU legislation took effect on May 25, 2018, GDPR is designed to protect the Personally Identifiable Information (PII) of European citizens. The scope of GDPR extends to citizens residing in EU member countries as well as citizens defined as residing in the European Economic Area.

Federal, State & Local Data Privacy, Handling, and Incident Reporting. The requirements for proper handling, security, and privacy of customer data can vary with each customer depending on federal, state, and /or local requirements. Certain states such as Florida impose laws such as the Florida Information Protection Act, or FIPA, requiring any entity that acquires, maintains, stores or uses personal information of individuals in the state to abide by specific requirements in regard to data breach reporting and records disposal. CentralSquare works closely with each customer to ensure that all data security requirements are addressed to satisfaction of the customer as well as state and local law.

Additional information regarding the CentralSquare Information Security Program can be obtained by contacting information.security@CentralSquare.com.

Analytics Product Security Overview

CentralSquare Technologies Analytics system provides security for Customer data through a layered approach. This security includes 1) Access controls to the application; 2) Secure infrastructure hosted at the hosting facility; 3) access limited to CentralSquare personnel with the required security approval. Analytics products, such as CrimeView and CrimeMapping, include data imported from the Customer's public safety systems (such as CAD and RMS).

CentralSquare Technologies Analytics products are deployed either on-premise at the Customer site or in a Cloud deployment. This document will primarily focus Cloud deployments. On-premise systems are protected by the customer through their physical and infrastructure security.

A common question regarding Analytics products is do these products store Criminal Justice Information (CJI) data. Analytics products does not directly query, display or store Criminal Justice Information (CJI) data. Analytics data imports exclude the import of CJI data. The imported data may include narrative fields referred to as "remarks." If the source data for remarks includes CJI data, CentralSquare recommends excluding remarks from the import process.

While the Analytics products do not import CJI, CentralSquare uses CJIS-level security for storage and access as a best practice for managing Customer operational data within Analytics.

CrimeView Security (including Subsystems such as CrimeView Analytics, FireView Analytics, CrimeView Dashboard, FireView Dashboard, Advanced Reporting Module, and NEARme)

1. Application security through CrimeView includes the following:
 - Role-based security restricts user access by agency, data sensitivity, and individual entities. The Customer's CrimeView system administrator controls user accounts and role-based security assignments.
 - CrimeView encryption of data in motion is through certified FIPS 140-2 encryption components. All data exchanged is encrypted CrimeView utilizes encryption components with the following FIPS 140-2 Certificates:
 - FIPS 140-2 Certificate 1337
 - FIPS 140-2 Certificate 1894Note: The encryption method is RSA, and the length is 2048 bit
 - The initial data load into CrimeView is extracted from the Customer's source system. This data is transmitted from the Customer's site utilizing an encrypted transfer tool. Once the initial data is loaded on the servers – either on-premise or in a Cloud deployment, a data update process is initiated between the Customer's source systems and the Analytics CrimeView servers.
 - CrimeView Cloud data is stored in Amazon Web Services (AWS) Government and encrypted at rest using Microsoft BitLocker.
 - CrimeView Cloud deployments hosted in AWS Government provide encryption through Bit-Locker (certified FIPS 140-2 encryption components – Microsoft BitLocker FIPS140-2-Jan2017-Certs-2932-2933-2934).

2. CrimeView is hosted from an Amazon Web Services (AWS) Government facility. Each of these facilities meet the stringent FBI CJIS Policy standards and guidelines with the following protection features on site:
 - Monitored by both fixed and pan-tilt/zoom security cameras
 - Protected by intrusion detection system
 - Two-factor authentication required for building access
 - Biometric iris authorization required for data center access
 - Extensive pre-employment background investigation process
 - On-site building security and data center monitoring staffed 24/7/365

The Cloud system infrastructure is managed and controlled by CentralSquare. CentralSquare Technologies currently hosts the Cloud CrimeView system at Amazon Web Services (AWS) Government.

- The AWS Government deployment is through AWS infrastructure as a service. AWS allocates infrastructure based upon a CentralSquare defined template and CentralSquare security authorized staff setup storage, OS, DBMS (SQL Server), applications and security.
 - CentralSquare manages application and security updates as well as Operating System, DBMS and application upgrades at both hosting sites.
 - Hosting facility personnel do not have access to the system and do not perform system setup or maintenance.
3. Cloud CrimeView access to implement and support the system is limited to personnel that have completed CentralSquare Technologies' CJIS compliant security approval process.
 - Access to the Cloud CrimeView infrastructure requires approved personnel to complete a layered secure login process that includes personally assigned passwords, advanced authentication to gain access to the CentralSquare Technologies network and secure access login to the applicable Cloud CrimeView domain, application and SQL Server database.
 - Pre-employment background check.
 - Training - Each of security approved employee successfully completed CJIS On-Line Security and Awareness training and testing. Their certifications are current and must be renewed every two years. In addition to CJIS required training, CentralSquare Technologies also does periodic training for security approved personnel on CentralSquare Technologies security policies.
 - Criminal background checks have been completed on each of these personnel by CentralSquare Technologies as part of employee screening and by one or more law enforcement agencies (CentralSquare Technologies Customers and in some cases, State law enforcement agencies).
 - Fingerprints – each of these personnel have been fingerprinted and their prints have been submitted to one or more law enforcement agencies for background check.
 - Security approved personnel are the same personnel that are utilized for supporting Customers with on premise deployments of CAD, Mobile, RMS and other CentralSquare products.

CrimeMapping Security

Crimemapping.com is hosted in the Microsoft Azure non-government cloud, where only non-sensitive data is stored. The Crimemapping architecture is like that of CrimeView, but Crimemapping data is presented to the public. Crimemapping.com records are first transmitted to the CrimeView AWS Government cloud then sent to the Crimemapping environment in Microsoft Azure. Hosted data at AWS and Azure is encrypted through Microsoft BitLocker and Microsoft FIPS 140-2 compliant encryption is utilized for data in transit (the same encryption components as CrimeView).

PROFESSIONAL SERVICES AGREEMENT
BETWEEN
THE CITY OF OAKLAND
AND CENTRALSQUARE TECHNOLOGIES

TABLE OF CONTENTS

1. Security.....5

2. Priority of Documents.....5

3. Conditions Precedent5

4. Statement of Work6

5. Initial Term6

6. City Requirements and Project Deliverables6

7. Contractor Warranty and Indemnification of Services6

8. Payment.....8

9. Reserved8

10. Proprietary or Confidential Information of the City9

11. Ownership of Results10

12. Amendments10

13. Limitation on Liability11

14. Security of and Access to City’s Information Technology Systems11

15. Indemnification11

16. Termination.....11

17. Dispute Resolution.....14

18. Implementation15

19. Bankruptcy16

20. Assignment16

21. Agents/Brokers16

22. Publicity17

23. Conflict of Interest17

24. Validity of Contracts.....17

25. Governing Law19

26. Headings19

27. Construction.....20

28. Waiver.....20

29. Independent Contractor.....20

30. Attorneys’ Fees20

31. Counterparts.....22

32. Remedies Cumulative.....22

33. Severability/Partial Invalidity22

34. Access22

35. Entire Agreement of the Parties.....22

36. Modification.....23

37. Notice.....23

38. No Third Party Beneficiary.....23

39. Survival.....24

40. Time is of the Essence.....24

41. Authority24

EXHIBITS

- Exhibit 1** **Statement of Work**
- Exhibit 2** **End User License Agreement and Support Terms**
- Exhibit 3** **Pricing and Payment Milestones**
- Exhibit 4** **Security Provisions**
 - a. **CentralSquare Cybersecurity Program Overview**
 - b. **CentralSquare Analytics Product Security Overview**
- Exhibit 6** **City Contract Compliance Provisions**
- Exhibit 7** **City Schedules**

This Agreement to provide Professional Services and Related Products as applicable and as set forth with specificity herein [“Agreement”] is by and between CentralSquare Tehnologies, a public safety software [INSERT NATURE OF ORGANIZATION AND WHERE ORGANIZED] located at 1000 Business Center Drive, Lake Mary, FL 32746 (“Contractor”) and the City of Oakland (“City”), a municipal corporation, located at One Frank H. Ogawa Plaza, Oakland, California 94612, who agree as follows:

RECITALS

This Agreement is made with reference to the following facts and objectives:

- A. **WHEREAS**, the City Council has authorized the City Administrator to enter into contracts for professional or specialized services if the mandates of Oakland City Charter Section 902(e) have been met; and
- B. **WHEREAS**, Contractor is the developer of public safety software products and related professional services [“Services”]; and
- C. **WHEREAS**, City is part of and provides information technology services to the various City departments, offices, and programs; and
- D. **WHEREAS**, City wishes to acquire Contractor’s Services and products as specifically set forth in this Agreement, including the Statement of Work [“SOW”] attached hereto.
- E. **WHEREAS**, the following Exhibits and Schedules are attached to and incorporated by reference into this Agreement:

- Exhibit 1 Statement of Work**
- Exhibit 2 Software Support Agreement**
- Exhibit 3 Pricing and Payment Milestones**
- Exhibit 4 CentralSquare Cybersecurity Program Overview**
- Exhibit 5 CentralSquare Analytics Product Security Overview**
- Exhibit 6 City Contract Compliance Provisions**
- Exhibit 7 City Schedules**

NOW THEREFORE, THE PARTIES TO THIS Agreement COVENANT AND AGREE AS FOLLOWS:

1. Security

a. Contractor's Security Program

In entering into this Agreement, City is relying upon Contractor's averment that it maintains a Security program for managing access to City data – particularly HIPAA and CJIS information which includes 1) a Pre-employment background check, 2) security training required by Federal CJIS regulations, and 3) criminal background checks/fingerprints required by Federal or State regulations. Contractor's Security program is detailed in the Security Provisions Exhibit 4 Contractor's Cybersecurity Program Overview and Exhibit 5 Contractor's Analytics Product Security Overview. In addition, Contractor avers to provide City the required documentation (such as the CJIS Security Addendum Certification form and VPN documents).

b. System Security

(i) Contractor shall at all times maintain and ensure that all of City's information technology systems which Contractor interfaces with or has access to remain secure and do not through any of Contractor's actions or lack of action thereof including, but not limited to, ransomware attacks upon Contractor, become vulnerable to breach, hacking into or in any way provide any unauthorized access to third parties. Contractor shall be liable for and indemnify City for all liabilities, claims, losses, damages and expenses, restorative or protective measures made necessary made necessary by any of the foregoing, including without limitation, reasonable attorney's fees.

(ii). Contractor shall not work on any City information technology system unless Contractor first contacts and obtains prior written authorization from the City's Director of Office of Information Technology, or his or her designee. Contractor warrants and represents that it will provide all information, reports, and data that fully informs the City with respect to any work, software deliverables, or products that the Contractor works on or which alter or affect the City's information technology systems, including without limitation, any source code and passwords necessary to access or make any such work, software, deliverables or products usable by the City.

c. Cloud Security

Contractor understands that, in contracting for Contractor's Cloud Storage Service is relying upon Contractor's representations that the methods and procedures it has in place to protect City's data as set forth in Exhibit X [INSERT CITE TO VENDOR'S SECURITY DOCUMENT], prevent unauthorized access to, corruption of and use of City's data including, but not limited to, ransomware attacks upon Contractor. Contractor further warrants and represents that it shall be liable for and fully indemnify the City for all liabilities, claims, losses, damages and expenses, including without limitation, reasonable attorney's fees, arising from claims against City due to a breach

of or other unauthorized access to the systems Contractor uses to provide City the services hereunder.

d. **Data Incidents.** Contractor shall implement and maintain a program for managing unauthorized disclosure of, access to, or use of City Data however they may occur (“Data Incidents”). In case of a Data Incident, or if Contractor confirms or suspects a Data Incident, Contractor shall: (1) promptly, and in any case within 24 hours, notify City by email, telephone, in person, or by other real-time, in-person communication; (2) cooperate with City and law enforcement agencies, where applicable, to investigate and resolve the Data Incident, including without limitation by providing reasonable assistance to City in notifying injured third parties; and (3) otherwise comply with applicable laws governing data breach notification and response. In addition, if the Data Incident results from Contractor’s other breach of this Agreement or negligent or unauthorized act or omission, including without limitation those of its subcontractors or other agents, Contractor shall (a) compensate City for any reasonable expense related to the Data Incident. Contractor shall give City prompt access to such records related to a Data Incident as City may reasonably request. City will treat such records as Contractor’s Confidential Information pursuant to **Section b., below**. Contractor is not required to give City access to records that might compromise the security of Contractor’s other customers.

In the event of a Data Incident, City will coordinate with Contractor on the content of any intended public statements or notices to the relevant authorities regarding the Data Incident.

This provision does not limit City’s other rights or remedies, if any, resulting from a Data Incident.

2. **Priority of Documents**

In the event of conflicting provisions as between the following documents, except as otherwise expressly stated, the provisions shall govern in the following order: the Amendments to this Agreement, in reverse chronological order of adoption, this Agreement and its Exhibits. The Exhibits shall govern in numerical order as set out in this Agreement.

3. **Conditions Precedent**

a Contractor must provide City with the following before the Agreement will become effective:

- (1). A copy of Contractor’s City of Oakland Business Tax License which must be kept current for the duration of the Agreement and shall be attached to this Agreement as part of Exhibit 6

(2). A completed set of the City of Oakland Schedules which shall be attached to this Agreement as Exhibit 7;

- b. Contractor and City must complete and agree upon and execute a Statement of Work before the Agreement will become effective and which shall be attached to this Agreement as Exhibit 1.

4. Statement of Work

Contractor avers and covenants to perform the services (“**Services**”) and provide the deliverables (“**Deliverables**”) specified in Exhibit 1, the Statement of Work including, but not limited to, the as requested or required Additional Items, Maintenance and Support for its Crimemapping.com and CrimeView Desktop products and providing its CrimeView Analytics product as a Software as a Service, all as set forth with specificity in the SOW

5. Term

This Agreement shall start when it is executed in full by the parties {“Effective Date”} and end on December 31, 2024. Should City decide, in its sole discretion, to exercise either or both of the authorized one-year extensions, and the parties mutually agree on the extensions, the Agreement may be extended until December 31, 2026.

6. City Requirements for Project Deliverables

Contractor avers and covenants to provide its Services and Deliverables which will include, but not be limited to, expanding the utility of Contractor’s CrimeView Analytics and crimemapping.com products, licensing and providing maintenance and support for those products and providing CrimeView Desktop to City as a Software as a Service, all as set forth in the SOW.

7. Contractor Warranty and Indemnification of Services

- a. Contractor will provide its software [“Software”] and Maintenance and Support Services under this Agreement “as is”, without warranty, and will support that “Software” from the date of live operational use (“Go Live”) in accordance with Contractor’s End User License Agreement and Software Support terms attached hereto as Exhibit 2. Subscription services are also provided “as is”, without warranty, and will be supported in accordance with the Contractor’s subscription terms in Exhibit 2
- b. Notwithstanding paragraph 7.a. above, Contractor warrants and represents that the Software does not contain any back door, time bomb, Trojan horse, worm, drop dead device, or other program or routine inserted and intended to provide a means of

unauthorized access to, or a means of disabling, or rendering the Software unusable or inoperable.

c. Contractor acknowledges that City is a provider of public and municipal services to the public and residents of the City of Oakland and that City's reliance on and use of Contractor's Deliverables will be vital to: (a) the business operations of the City; (b) the orderly and efficient provision of public and municipal services by the City; and (c) the health and safety of City's residents; and therefore, that any unauthorized interruption of City's business and operations could result in substantial liability to City. In recognition of City's status as a provider of such public and municipal services, Contractor warrants and represents that Contractor shall not at any time during the term of this Agreement and thereafter render the Software unusable or inoperable, or otherwise disable the Contractor's software, take possession of the Software or if any, the Hardware provided to City by Contractor or Contractor's subcontractors or in any way deliberately take actions limiting Contractor's liability under this Agreement. If Contractor takes any such actions, Contractor shall be liable for and indemnify City for all liabilities, claims, losses, damages and expenses, including without limitation, reasonable attorney's fees, arising from Contractor's actions.

d. The Services and Deliverables (a) will conform in all material respects to the Specifications

e. Contractor represents that it will use commercially reasonable efforts, including appropriate testing, to ensure that the Software does not contain viruses, contaminants, or other harmful code that may harm the Software, City systems or other City software.

f. Contractor represents that it owns or has the unencumbered right to license to City, the Deliverables and all results of Services delivered to City hereunder, including all required Intellectual Property Rights therein.

g. Contractor represents that it has the requisite experience, certifications, skills and qualifications necessary to perform the Services in: (i) a timely, competent, and professional manner, and (ii) accordance with applicable governmental requirements, statutes, regulations, rules and ordinances including, without limitation, applicable data privacy laws and regulations ("Law");

h. Contractor further warrants and represents that the methods and procedures it has in place to protect City's data as set forth in Exhibit 4 [Central Square Security Overview letter], prevent unauthorized access to, corruption of and use of City's data, Contractor further warrants and represents that, subject to the coverage limits of its Cyber Insurance, it shall be liable for and fully indemnify the City for all liabilities, claims, losses, damages and expenses, including without limitation, reasonable attorney's fees, arising from claims against City due to a breach of or unauthorized access to the systems Contractor uses to provide City the services hereunder.

i. EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES MADE IN THIS AGREEMENT, THE CONTRACTOR MAKES NO REPRESENTATION, ACKNOWLEDGEMENT, CONDITION OR WARRANTY OF

ANY KIND WHATSOEVER UNDER THIS AGREEMENT OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY STATUTORY, EXPRESS, IMPLIED OR OTHER WARRANTIES OR ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE REGARDING ANY SERVICES, DELIVERABLE OR ANY OTHER PRODUCT DELIVERED TO THE CITY UNDER THIS AGREEMENT.

8. **Payments.**

City shall pay Contractor the CrimeView Analytics, CrimeView Desktop and Crimemapping Services fees along with the annual Software License Fees and the Additional Items Reserve for those services City requests Contractor to provide, the not to exceed fees set forth in Exhibit 3 [Pricing and Payment Milestones].

9. **[RESERVED]**

10. **Proprietary or Confidential Information**

10.1 Confidentiality Obligations. Confidential Information shall mean all proprietary or confidential information disclosed or made available by the other Party pursuant to this Agreement that is identified as confidential or proprietary at the time of disclosure or is of a nature that should reasonably be considered to be confidential, and includes, but is not limited to, the terms and conditions of this Agreement, and all business, technical and other information (including without limitation, all product, services, financial, marketing, engineering, research and development information, product specifications, technical data, data sheets, software, inventions, processes, training manuals, know-how and any other information or material), disclosed from time to time by the disclosing Party to the receiving Party, directly or indirectly in any manner whatsoever (including without limitation, in writing, orally, electronically, or by inspection); provided, however, that Confidential Information shall not include the Content that is intended to be published on the website(s) of either Party.

10.2 Each Party agrees to keep confidential and not disclose to any third party and to use only for purposes of performing or as otherwise permitted under this Agreement, any Confidential Information. The receiving Party shall protect the Confidential Information using measures similar to those it takes to protect its own confidential and proprietary information of a similar nature but not less than reasonable measures. Each Party agrees not to disclose the Confidential Information to any of its Representatives except those who are required to have the Confidential Information in connection with this Agreement and then only if such Representative is either subject to a written confidentiality agreement or otherwise subject to fiduciary obligations of confidentiality that cover the confidential treatment of the Confidential Information.

10.3 Exceptions.

The obligations of this Section 10 shall not apply if the receiving Party can prove by

appropriate documentation, where appropriate, that such Confidential Information (i) was known to the receiving Party as shown by the receiving Party's files at the time of disclosure thereof, (ii) was already in the public domain at the time of the disclosure thereof, (iii) entered the public domain through no action of the receiving Party subsequent to the time of the disclosure thereof, (iv) is or was independently developed by the Contractor without access to or use of the Confidential Information; (v) was provided to the Contractor by a third party who, to the best of the Contractor's knowledge, was not bound by any confidentiality obligation related to such Confidential Information; or (vi) is required by law or government order to be disclosed by the receiving Party, provided that the receiving Party shall (i) notify the disclosing Party in writing of such required disclosure as soon as reasonably possible prior to such disclosure, (ii) use its commercially reasonable efforts at its expense to cause such disclosed Confidential Information to be treated by such governmental authority as trade secrets and as confidential.

10.4 Contractor acknowledges that City is subject to public disclosure laws and that City will comply with requests for information ("RFI"), as it is required to do under the federal Freedom of Information Act, California Public Records Act, City of Oakland Sunshine Act or judicial or administrative court order. Contractor acknowledges that an RFI may pertain to any and all documentation associated with City's use of Contractor's Services. Contractor further acknowledges that it is obligated to assist and cooperate with City by producing all documentation that City requests as responsive to the RFI so that City may comply with its statutory obligations. City agrees to give Contractor as timely written notice as possible of the RFI such that Contractor may oppose the RFI or exercise such other rights at law as Contractor believes it has. However, Contractor must produce to City all documents City requests as RFI responsive and City will comply with the RFI unless, within the time frame established by the statute, judicial or court order under which the RFI is made, Contractor procures a Temporary Restraining Order or similar injunctive relief from a court or other tribunal of competent jurisdiction ordering City not to comply with the RFI pending final determination of Contractor's protest of the RFI. Contractor further agrees to accept City's tender of defense and to defend City and pay all City costs of defense in any litigation brought against City with respect to City not complying with an RFI that Contractor protests and will hold City harmless against any claims, attorneys' fees, damages, fines, judgments, or administrative penalties, which may arise from any such actions.

11. Ownership of Results

Excluding the Contractor's intellectual property, or if applicable, any subcontractor intellectual property, any interest of Contractor or its Subcontractors, in specifications, studies, reports, memoranda, computation documents in drawings, plans, sheets prepared by Contractor or its Subcontractors under this Agreement shall be assigned and transmitted to the City. However, Contractor may retain and use copies for reference and as documentation of its experience and capabilities.

12. Amendments

Changes to this Agreement will only be made by mutually agreed upon Amendments in writing.

13. Limitation on Liability

(a) Either party's liability to the other party for any and all liabilities, claims or damages arising out of or relating to this Agreement [Direct Damages], howsoever caused and regardless of the legal theory asserted, including breach of contract or warranty, tort, strict liability, statutory liability or otherwise, shall not, in the aggregate, exceed twice the total value of this Agreement as set forth in Exhibit 3 [Pricing and Payment Milestones].

(b) IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY PUNITIVE, EXEMPLARY, SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOST PROFITS, LOST BUSINESS OPPORTUNITIES, LOSS OF USE OR EQUIPMENT DOWN TIME, AND LOSS OF OR CORRUPTION TO DATA) ARISING OUT OF OR RELATING TO THIS AGREEMENT, REGARDLESS OF THE LEGAL THEORY UNDER WHICH SUCH DAMAGES ARE SOUGHT, AND EVEN IF THE PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

(c) This limitation of liability shall not apply to Contractor's [Indemnification] obligations as set forth in this Agreement.

14. Reserved**15. Indemnification****(a) General Indemnification.**

Notwithstanding any other provision of this Agreement, Contractor shall indemnify and hold harmless (and at City's request, defend) City, and each of their respective Councilmembers, officers, partners, agents, and employees (each of which persons and organizations are referred to collectively herein as "Indemnitees" or individually as "Indemnatee") from and against any and all liabilities (of every kind, nature and description), claims, lawsuits, losses, damages, demands, debts, liens, costs, judgments, obligations, administrative or regulatory fines or penalties, damages, (incidental or consequential) costs, actions or causes of action, and expenses, including reasonable attorneys' fees, (collectively referred to herein as "Actions") caused by or arising out of:

- (i) A claim for personal injury (including death) or property damage to the extent based on the strict liability or caused by any negligent act, error or omission of Contractor;

- (ii) Unauthorized use or disclosure by Contractor of Confidential Information as provided in Section 10 above.

(b) Proprietary Rights Indemnity. Contractor shall indemnify, defend, save and hold harmless Indemnitees from any and all actions arising out of third party claims that the Contractor's Services, or Software, if any infringes upon or violates the Intellectual Property Rights of a third party. If the Services or Software will become the subject of an Action or claim of infringement or violation of the Intellectual Property Rights of a third party, Contractor may, in addition to its obligation to defend and indemnify City hereunder, in its discretion, and at Contractor's sole expense: (1) procure for City the right to continue using the Services or Software; or (2) replace or modify the Services or Software so that no infringement or other violation of Intellectual Property Rights occurs, if City determines that: (A) such replaced or modified Services or Software will operate in all material respects in conformity with the then-current specifications for the Services or Software; and (B) City's use of the Services or Software is not impaired thereby. Contractor's obligations under this Agreement will continue uninterrupted with respect to the replaced or modified Services or Software as if it were the original Software. If Contractor concludes in its sole judgement that none of the foregoing options are commercially reasonable, and the City's use of the Contractor's Services or Software is permanently enjoined this Agreement and the license granted herein shall terminate.

(c) Contractor shall have no duty under Section 15 (b) and shall not be liable for any Actions arising from;

- (1) modifications made to Contractor's Software or the Services by the City unless the City has made such modifications at the request or direction of Contractor;
- (2) the Contractor having been required to conform to all or part of specific product designs of the City, provided that the Contractor has informed the City that any such requirement to conform may result in a claim under clause 16(b);
- (3) the use by the City of Contractor's Software or Services or any part of them with programs, hardware, or software supplied by other parties, unless the Contractor has represented to the City that its Software or Services or any part of them are designated for use with such other programs, hardware, or software;
- (4) use of Contractor's Software or Services or any part of them by the City in a manner contrary to the Contractor's specifications and/or documentation provided by or through the Contractor and accepted by the City;
- (5) use of Contractor's Software or Services or any part of them by the City on any hardware for which the Software or Services or any part of them was not designed; or
- (6) the City not using corrections to the Software or Services or any part of them made known and available by the Contractor.

(d) For the purposes of the indemnification obligations set forth herein, the term "Contractor" includes, without limitation, Contractor, its officers, directors, employees, representatives, agents, servants, sub consultants, and subcontractors.

- (e) Contractor acknowledges and agrees that it has an immediate and independent obligation to indemnify and defend Indemnitees from any Action which potentially falls within this Indemnification provision, which obligation shall arise at the time an Action is tendered to Contractor by City and continues at all times thereafter, without regard to any alleged or actual contributory negligence of any Indemnitee. Notwithstanding anything to the contrary contained herein, if a claim, lawsuit or liability results from or is contributed to by the actions or omissions of an Indemnitee, Contractor's liability under this provision shall be reduced to the extent of such actions or omissions based upon the principle of comparative fault.
- (f) City shall give Contractor prompt written notice of any Action and shall fully cooperate with Contractor in the defense and all related settlement negotiations to the extent that cooperation does not conflict with City's interests. Notwithstanding the foregoing, City shall have the right, if Contractor fails or refuses to defend City with Counsel acceptable to City, to engage its own counsel for the purposes of participating in the defense. In addition, City shall have the right to withhold payments due Contractor in the amount of reasonable defense costs actually incurred. In no event shall Contractor agree to the settlement of any claim described herein without the prior written consent of City.
- (g) All of Contractor's Indemnification obligations hereunder are intended to apply to the fullest extent permitted by law (including, without limitation, California Civil Code Section 2782) and shall survive the expiration or sooner termination of this Agreement.
- (h) Contractor's Indemnification obligations hereunder shall not be limited by the City's insurance requirements contained in Schedule Q hereof, or by any other provision of this Agreement.

16. **Termination**

- (a) **Termination for Breach.** If Contractor breaches any material obligation under this Agreement and fails to cure the breach within 30 days of receipt of written notice from City of said breach, City may terminate the Agreement and, subject to the Limitation on Liability (Section 13), recover all Direct Damages it incurs as a result of Contractor's breach.
- (b) Contractor may terminate this Agreement if City breaches a material provision of the Agreement and does not cure the breach within 30 days of written notice from Contractor of said breach. In such event, Contractor will be entitled to payment of all fees for Services or Deliverables the City has Accepted but not paid Contractor up to the date of termination.
- (c) **Bankruptcy.** Either party may immediately terminate this Agreement if (i) the other party files a petition for bankruptcy or has filed against it an involuntary petition for bankruptcy which is not dismissed within 60 days of its filing, (ii) a court has appointed a receiver, trustee, liquidator or custodian of it or of all or a

substantial part of the other party's property, (iii) the other party becomes unable, or admits in writing its inability, to pay its debts generally as they mature, or (iv) the other party makes a general assignment for the benefit of its or any of its creditors.

- (d) Termination for Convenience by City. City may terminate this Agreement for any reason at any time upon not less than sixty (60) days' prior written notice to Contractor. After the date of such termination notice, Contractor shall not perform any further services or incur any further costs claimed to be reimbursable under this Agreement, any Purchase Order, Change Order, or Change Notice without the express prior written approval of City. As of the date of termination, City shall pay Contractor for Services or Deliverables the City has Accepted but not paid Contractor
- (e) Transition Services after termination. In connection with the expiration or other termination of this Agreement or the expiration of this Agreement, Contractor may provide transition services as requested by City. Contractor shall provide a quotation to City for any transition services, and shall not be obligated to provide any services until both parties have mutually agreed in writing to such quotation.
- (f) Effect of Termination. Upon termination of this Agreement, City shall remove all Contractor Software from its computer system and certify in writing to Contractor that it has destroyed all Contractor Software and its associated documentation. Any City data in Contractor's possession shall either be returned to the City or destroyed as directed by the City.

17. Dispute Resolution

- a. If dispute or disagreement among the Parties arises with respect to either Party's performance of its obligations hereunder, or any provision of or interpretation of the Agreement, the Parties agree in good faith to attempt to resolve such dispute or disagreement (a "Dispute") prior to submitting the Dispute to mediation, arbitration or litigation in accordance with this Section 17. Such resolution efforts shall involve the City Administrator of the City of Oakland and an executive officer of Contractor, together with such other persons as may be designated by either Party.
- b. Any Party may commence said resolution efforts by giving notice, in writing, to any other Party. Such notice shall include at least a description of the Dispute and any remedial action that the Party commencing the resolution procedure asserts would resolve the Dispute. Upon receiving such notice, the Party against whom the Dispute is brought shall respond in writing within five (5) Business Days. The Parties shall then meet and confer in a good faith attempt to resolve the Dispute.

c If the Dispute has not been resolved within ten (10) Business Days after the Subsection 17.b. notice is given, said period to be extended by the parties' mutual agreement and, unless the Party initiating the Dispute does not wish to pursue its rights relating to such Dispute or desires to continue the Pre-Mediation Dispute Resolution, then such Dispute will be automatically submitted to mediation. The mediation will be conducted in Alameda County by a single mediator selected by the Parties to the Dispute by mutual agreement or by the use of the Commercial Arbitration Rules of the American Arbitration Association for selecting an Arbitrator ["AAA RULES"] The Parties to the Dispute shall evenly share the fees and costs of the mediator. The mediator shall have twenty (20) Business Days from the submission to mediation to attempt to resolve such Dispute. If the Dispute is not resolved within that time period, the parties will be entitled to pursue such matter by demanding arbitration under the AAA RULES or instituting litigation.

18. **Implementation**

A mutually agreed upon Project Schedule will be developed for implementation of the Project under this Agreement as defined in the Statement of Work. The Project Schedule will define timelines and responsibilities of each Party and may be modified at the mutual agreement of the Parties.

19. **Bankruptcy**

All rights and licenses granted to City pursuant to this Agreement are, and shall be deemed to be, for purposes of Section 365(n) of the U.S. Bankruptcy Code, licenses of rights to "intellectual property" as defined under Section 101 of the U.S. Bankruptcy Code. In a bankruptcy or insolvency proceeding involving Contractor, the parties agree that City, as licensee of such rights, shall retain and fully exercise all of its rights and elections under the U.S. Bankruptcy Code, and the provisions thereof shall apply notwithstanding conflict of law principles. The parties further agree that, in the event of the commencement of a bankruptcy or insolvency proceeding by or against Contractor under the U.S. Bankruptcy Code, City shall be entitled to a complete duplicate of any such intellectual property, including the source code for Contractor's Licensed Software which Contractor has placed in escrow as required under this Agreement and all embodiments of such intellectual property, to which City would otherwise be entitled under this Agreement, and the same, if not already in City's possession, shall be promptly delivered to City (a) upon any such commencement of a bankruptcy proceeding upon written request therefore by City, unless Contractor elects to continue to perform all of its obligations under this Agreement, or (b) if not delivered under (a) above, upon rejection of this Agreement by or on behalf of Contractor upon written request therefore by City. If, in a bankruptcy or insolvency proceeding involving Contractor, the provisions of the U.S. Bankruptcy Code referenced above are determined not to apply, City shall nevertheless be entitled to no less than the protection offered by the provisions of the U.S. Bankruptcy Code with respect to its entitlement to and rights to the use and possession of all intellectual property to which City has been granted rights under this Agreement notwithstanding the bankruptcy or insolvency of Contractor.

20. Assignment

Contractor shall not assign or otherwise transfer any rights, duties, obligations or interest in this Agreement or arising hereunder to any person, persons, entity or entities whatsoever without the prior written consent of **the City Attorney and City Administrator or their respective designees, which shall not be unreasonably withheld. City's consent to any assignment shall be conditioned upon retaining all rights it has at law against Contractor as Assignor.** Any attempt to assign or transfer without such prior written consent shall be void. Consent to any single assignment or transfer shall not constitute consent to any further assignment or transfer. In the event that Contractor assigns this Agreement in compliance with this provision, this Agreement and all of its provisions shall inure to the benefit of and become binding upon the parties and the successors and permitted assigns of the respective parties.

21. Agents/Brokers

Contractor warrants that Contractor has not employed or retained any subcontractor, agent, company or person other than bona fide, full-time employees of Contractor working solely for Contractor, to solicit or secure this Agreement, and that Contractor has not paid or agreed to pay any subcontractor, agent, company or persons other than bona fide employees any fee, commission, percentage, gifts or any other consideration, contingent upon or resulting from the award of this Agreement. For breach or violation of this warranty, the City shall have the right to rescind this Agreement without liability or, in its discretion, to deduct from the Agreement price or consideration, or otherwise recover, the full amount of such fee, commission, percentage or gift.

22. Publicity

Any publicity generated by Contractor for the project funded pursuant to this Agreement, during the term of this Agreement or for one year thereafter, must be approved by the City in advance and will make reference to the contribution of the City of Oakland in making the project possible. The words "City of Oakland" will be explicitly stated in all pieces of publicity, including but not limited to flyers, press releases, posters, brochures, public service announcements, interviews and newspaper articles.

City staff will be available whenever possible at the request of Contractor to assist Contractor in generating publicity for the project funded pursuant to this Agreement. Contractor further agrees to cooperate with authorized City officials and staff in any City-generated publicity or promotional activities undertaken with respect to this project.

23. Conflict of Interest

(a) Contractor

The following protections against conflict of interest will be upheld:

- (1) Contractor certifies that no member of, or delegate to the Congress of the United States shall be permitted to share or take part in this Agreement or in any benefit arising there from.
- (2) Contractor certifies that no member, officer, or employee of the City or its designees or agents, and no other public official of the City who exercises any functions or responsibilities with respect to the programs or projects covered by this Agreement, shall have any interest, direct or indirect in this Agreement, or in its proceeds during his/her tenure or for one year thereafter.
- (3) Contractor shall immediately notify the City of any real or possible conflict of interest between work performed for the City and for other clients served by Contractor.
- (4) Contractor warrants and represents, to the best of its present knowledge, that no public official or employee of City who has been involved in the making of this Agreement, or who is a member of a City board or commission which has been involved in the making of this Agreement whether in an advisory or decision-making capacity, has or will receive a direct or indirect financial interest in this Agreement in violation of the rules contained in California Government Code Section 1090 *et seq.*, pertaining to conflicts of interest in public contracting. Contractor shall exercise due diligence to ensure that no such official will receive such an interest.
- (5) Contractor further warrants and represents, to the best of its present knowledge and excepting any written disclosures as to these matters already made by Contractor to City, that (1) no public official of City who has participated in decision-making concerning this Agreement or has used his or her official position to influence decisions regarding this Agreement, has an economic interest in Contractor or this Agreement, and (2) this Agreement will not have a direct or indirect financial effect on said official, the official's spouse or dependent children, or any of the official's economic interests. For purposes of this paragraph, an official is deemed to have an "economic interest" in any (a) for-profit business entity in which the official has a direct or indirect investment worth \$2,000 or more, (b) any real property in which the official has a direct or indirect interest worth \$2,000 or more, (c) any for-profit business entity in which the official is a director, officer, partner, trustee, employee or manager, or (d) any source of income or donors of gifts to the official (including nonprofit entities) if the income totaled more than \$500 in the previous 12 months, or value of the gift totaled more than \$350 the previous year. Contractor agrees to promptly disclose to City in writing any information it may receive concerning any such potential conflict of interest.

Contractor's attention is directed to the conflict of interest rules applicable to governmental decision-making contained in the Political Reform Act (California Government Code Section 87100 et seq.) and its implementing regulations (California Code of Regulations, Title 2, Section 18700 et seq.).

- (6) Contractor understands that in some cases Contractor or persons associated with Contractor may be deemed a "City officer" or "public official" for purposes of the conflict of interest provisions of Government Code Section 1090 and/or the Political Reform Act. Contractor further understands that, as a public officer or official, Contractor or persons associated with Contractor may be disqualified from future City contracts to the extent that Contractor is involved in any aspect of the making of that future contract (including preparing plans and specifications or performing design work or feasibility studies for that contract) through its work under this Agreement.
- (7) Contractor shall incorporate or cause to be incorporated into all subcontracts for work to be performed under this Agreement a provision governing conflict of interest in substantially the same form set forth herein.

(b) No Waiver

Nothing herein is intended to waive any applicable federal, state or local conflict of interest law or regulation.

(c) Remedies and Sanctions

In addition to the rights and remedies otherwise available to the City under this Agreement and under federal, state and local law, Contractor understands and agrees that, if the City reasonably determines that Contractor has failed to make a good faith effort to avoid an improper conflict of interest situation or is responsible for the conflict situation, the City may (1) suspend payments under this Agreement, or (2) terminate this Agreement, (3) require reimbursement by Contractor to the City of any amounts disbursed under this Agreement. In addition, the City may suspend payments or terminate this Agreement whether or not Contractor is responsible for the conflict of interest situation.

24. Validity of Contracts

The Oakland City Council must approve all Agreements greater than \$15,000. This Agreement shall not be binding or of any force or effect until signed by the City Manager or his or her designee and approved as to form and legality by the City Attorney or his or her designee.

25. Governing Law

This Agreement shall be governed and construed in accordance with the laws of the State of California, without reference to its conflicts of laws principles. Any action or proceeding to enforce the terms of this Agreement shall be brought in the courts of Alameda County, Oakland, California and each party agrees to waive any objections to personal jurisdiction and venue in the courts of Alameda County, Oakland, California.

26. Headings

Headings and captions used to introduce Sections and paragraphs of this Agreement are for convenience, only, and have no legal significance.

27. Construction

- (a) Acceptance or acquiescence in a prior course of dealing or a course of performance rendered under this Agreement or under any Change Order, or Change Notice, shall not be relevant in determining the meaning of this Agreement even though the accepting or acquiescing party has knowledge of the nature of the performance and opportunity for objection.
- (b) The language in all parts of this Agreement and any Purchase Order, Change Order, or Change Notice, shall in all cases be construed in whole, according to its fair meaning, and not strictly for or against, either Contractor, City regardless of the drafter of such part.

28. Waiver

No covenant, term, or condition of this Agreement may be waived except by written consent of the party against whom the waiver is claimed and the waiver of any term, covenant or condition of this Agreement shall not be deemed a waiver of any subsequent breach of the same or any other term, covenant or condition of this Agreement.

29. Independent Contractor

- (a) Rights and Responsibilities

It is expressly agreed that in the performance of the services necessary to carry out this Agreement, Contractor shall be, and is, an independent contractor, and is not an employee of the City. Contractor acknowledges and agrees that all of Contractor's employees and subcontractors are under the sole direction and control of Contractor and City shall have no authority over or responsibility for such employees and subcontractors of Contractor. Contractor has and shall retain the right to exercise sole direction and supervision of the services, and full control over the employment, direction, compensation and discharge of all persons

assisting Contractor in the performance of Contractor's services hereunder. Contractor shall be solely responsible for all matters relating to the payment of his/her employees, including compliance with social security, withholding and all other regulations governing such matters, and shall be solely responsible for Contractor's own acts and those of Contractor's subordinates and employees. Contractor will determine the method, details and means of performing the services described in **EXHIBIT 1**.

(b) Contractor's Qualifications

Contractor represents that Contractor has the qualifications and skills necessary to perform the services under this Agreement in a competent and professional manner without the advice or direction of the City. This means Contractor is able to fulfill the requirements of this Agreement. Failure to perform all of the services required under this Agreement will constitute a material breach of the Agreement and may be cause for termination of the Agreement. Contractor has complete and sole discretion for the manner in which the work under this Agreement is performed. Contractor shall complete and submit to City, Schedule M-Independent Contractor Questionnaire, prior to the execution of this Agreement.

(c) Payment of Income Taxes

Contractor is responsible for paying, when due, all income taxes, including estimated taxes, incurred as a result of the compensation paid by the City to Contractor for services under this Agreement. On request, Contractor will provide the City with proof of timely payment. Contractor agrees to indemnify the City for any claims, costs, losses, fees, penalties, interest or damages suffered by the City resulting from Contractor's failure to comply with this provision.

(d) Non-Exclusive Relationship

Contractor may perform services for, and contract with, as many additional clients, persons or companies as Contractor, in his or her sole discretion, sees fit.

(e) Tools, Materials and Equipment

Contractor will supply all tools, except those tools, materials, equipment specified herein, if any, required to perform the services under this Agreement.

(f) Cooperation of the City

The City agrees to comply with all reasonable requests of Contractor necessary to the performance of Contractor's duties under this Agreement.

(g) Extra Work

Contractor will do no extra work under this Agreement without first receiving prior written authorization from the City.

30. Attorneys' Fees

If either party commences an action or proceeding to determine or enforce its rights hereunder, the prevailing party shall be entitled to recover from the losing party all expenses reasonably incurred, including court costs, reasonable attorneys' fees and costs of suit as determined by the court.

31. Counterparts

This Agreement may be executed in any number of identical counterparts, any set of which signed by both parties shall be deemed to constitute a complete, executed original for all purposes.

32. Remedies Cumulative

The rights and remedies of either Party provided in this Agreement shall not be exclusive and are in addition to any other rights and remedies provided by law, including the California Uniform Commercial Code.

33. Severability/Partial Invalidity

If any term or provision of this Agreement, or the application of any term or provision of this Agreement to a particular situation, shall be finally found to be void, invalid, illegal or unenforceable by a court of competent jurisdiction, then notwithstanding such determination, such term or provision shall remain in force and effect to the extent allowed by such ruling and all other terms and provisions of this Agreement or the application of this Agreement to other situation shall remain in full force and effect.

Notwithstanding the foregoing, if any material term or provision of this Agreement or the application of such material term or condition to a particular situation is finally found to be void, invalid, illegal or unenforceable by a court of competent jurisdiction, then the Parties hereto agree to work in good faith and fully cooperate with each other to amend this Agreement to carry out its intent.

34. Access

Access to City's premises by Contractor shall be subject to the reasonable security and operational requirements of City. To the extent that Contractor's obligations under this Agreement or any Purchase Order, Change Order, or Change Notice, require the performance

of Services or Work by Contractor on City’s property or property under City's control, Contractor agrees:

- (i) to accept full responsibility for performing all Services or work in a safe manner so as not to jeopardize the safety of City's personnel, property, or members of the general public; and
- (ii) to comply with and enforce all of City's applicable regulations, policies, and procedures including, without limitation, those with respect to security, access, safety and fire protection, City’s policy against sexual harassment, and all applicable state and municipal safety regulations, building codes or ordinances.

35. Entire Agreement of the Parties

This Agreement supersedes any and all Agreements, either oral or written, between the parties with respect to the rendering of services by Contractor for the City and contains all of the representations, covenants and Agreements between the parties with respect to the rendering of those services. Each party to this Agreement acknowledges that no representations, inducements, promises or Agreements, orally or otherwise, have been made by any party, or anyone acting on behalf of any party, which are not contained in this Agreement, and that no other Agreement, statement or promise not contained in this Agreement will be valid or binding.

36. Modification

Any modification of this Agreement will be effective only if it is in a writing signed by all parties to this Agreement.

37. Notices

If either party shall desire or be required to give notice to the other, such notice shall be given in writing, via facsimile and concurrently by prepaid U.S. certified or registered postage, addressed to recipient as follows:

(City of Oakland) _____

Oakland Police Department
Nicole Freeman
455 7th Street, 2nd Floor
Oakland, CA 94607

(Contractor)

CentralSquare Technologies
Attn: Legal/Contracts
1000 Business Center Drive
Lake Mary, FL 32746

Any party to this Agreement may change the name or address of representatives for purpose of this Notice paragraph by providing written notice to all other parties ten (10) business days before the change is effective.

38. No Third Party Beneficiary

This Agreement shall not be construed to be an agreement for the benefit of any third Party or parties, and no third party or parties shall have any claim or right of action under this Agreement

39. Survival

Sections (2, 6, 7, 8, 9, 10, 13, 14, 15, 16, 17, 20, 25, 30 and 38) of this Agreement, along with any other provisions which by their terms survive, shall survive the expiration or termination of this Agreement.

40. Time is of the Essence

The Special Circumstances of this Agreement require each Party's timely performance of its obligations under this Agreement. Each Party agrees perform its applicable obligations for implementation in accordance with the mutually agreed upon Project Schedule.

41. Authority

Each individual executing this Agreement or any Purchase Order, Change Order or Change Notice, hereby represents and warrants that he or she has the full power and authority to execute this Agreement or such Purchase Order, Change Order or Change Notice, on behalf of the named party such individual purports to bind.

SO AGREED:

City of Oakland,
a municipal corporation

CentralSquare Software Systems

(City Administrator’s Office) (Date)

(Signature) (Date)

(Department Head Signature) (Date)

00200550

Business Tax Certificate No.

Approved as to form and legality:

Resolution Number

(City Attorney’s Office Signature) (Date)

ATTACHMENT A

Schedule Q
INSURANCE REQUIREMENTS
Professional/Cyber Liability Exposures
(Revised 1/13/2017:dkg)

a. General Liability, Automobile, Workers' Compensation and Professional Liability

Contractor shall procure, prior to commencement of service, and keep in force for the term of this contract, at Contractor's own cost and expense, the following policies of insurance or certificates or binders as necessary to represent that coverage as specified below is in place with companies doing business in California and acceptable to the City. The insurance shall at a minimum include:

- i. **Commercial General Liability insurance** shall cover bodily injury, property damage and personal injury liability for premises operations, independent contractors, products-completed operations personal & advertising injury and contractual liability. Coverage shall be at least as broad as Insurance Services Office Commercial General Liability coverage (occurrence Form CG 00 01)

Limits of liability: Contractor shall maintain commercial general liability (CGL) and, if necessary, commercial umbrella insurance with a limit of not less than \$2,000,000 each occurrence. If such CGL insurance contains a general aggregate limit, either the general aggregate limit shall apply

separately to this project/location or the general aggregate limit shall be twice the required occurrence limit. Such limits may be met through a combination of primary and umbrella/excess coverages.

- ii. **Automobile Liability Insurance.** Contractor shall maintain automobile liability insurance for bodily injury and property damage liability with a limit of not less than \$1,000,000 each accident. Such insurance shall cover liability arising out of any auto (including owned, hired, and non-owned autos). Coverage shall be at least as broad as Insurance Services Office Form Number CA 0001.
- iii. **Worker's Compensation insurance** as required by the laws of the State of California, with statutory limits, and statutory coverage may include Employers' Liability coverage, with limits not less than \$1,000,000 each accident, \$1,000,000 policy limit bodily injury by disease, and \$1,000,000 each employee bodily injury by disease. The Contractor certifies that he/she is aware of the provisions of section 3700 of the California Labor Code, which requires every employer to provide Workers' Compensation coverage, or to undertake

self-insurance in accordance with the provisions of that Code. The Contractor shall comply with the provisions of section 3700 of the California Labor Code before commencing performance of the work under this Agreement and thereafter as required by that code.

- iv. ***Technology Professional Liability (Errors and Omissions) OR Cyber Liability Insurance*** appropriate to the Consultant's profession, with limits not less than **\$2,000,000** per occurrence or claim, **\$2,000,000** aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Consultant in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

b. Terms Conditions and Endorsements

The aforementioned insurance shall be endorsed and have all the following conditions:

- i. Insured Status (Additional Insured): Contractor shall provide additional insured status including the City of Oakland, its Councilmembers, directors, officers, agents, employees and volunteers as insured's under the Commercial General Liability policy. General liability coverage can be provided in the form of an endorsement to the Consultant's insurance (at least as broad as ISO Form CG 20 10 11 85 or **both** CG 20 10, CG 20 26, CG 20 33, or CG 20 38; **and** CG 20 37 forms if later revisions used). A STATEMENT OF ADDITIONAL INSURED STATUS ON THE ACORD INSURANCE CERTIFICATE FORM IS INSUFFICIENT AND WILL BE REJECTED AS PROOF OF MEETING THIS REQUIREMENT; and
- ii. Coverage afforded on behalf of the City, Councilmembers, directors, officers, agents, employees and volunteers shall be primary insurance. Any other insurance available to the City Councilmembers, directors, officers, agents, employees and volunteers under any other policies shall be excess insurance (over the insurance required by this Agreement); and
- iii. Cancellation Notice: Each insurance policy required by this clause shall provide that coverage shall not be canceled, except with notice to the Entity; and

- iv. Certificate holder is to be the same person and address as indicated in the “Notices” section of this Agreement; and
- v. Insurer shall carry insurance from admitted companies with an A.M. Best Rating of A:VII, or better.

c. Insurance Interpretation

All endorsements, certificates, forms, coverage and limits of liability referred to herein shall have the meaning given such terms by the Insurance Services Office as of the date of this Agreement.

d. Proof of Insurance

Contractor will be required to provide proof of all insurance required for the work prior to execution of the contract. Failure to provide the insurance proof requested or failure to do so in a timely manner shall constitute ground for rescission of the contract award.

e. Subcontractors

Should the Contractor subcontract out the work required under this agreement, they shall include all subcontractors as insured's under its policies or shall maintain separate certificates and endorsements for each subcontractor. As an alternative, the Contractor may require all subcontractors to provide at their own expense evidence of all the required coverages listed in this Schedule. If this option is exercised, both the City of Oakland and the Contractor shall be named as additional insured under the subcontractor's General Liability policy. All coverages for subcontractors shall be subject to all the requirements stated herein. The City reserves the right to perform an insurance audit during the course of the project to verify compliance with requirements.

f. Waiver of Subrogation

Contractor waives all rights against the City of Oakland and its Councilmembers, officers, directors, employees and volunteers for recovery of damages to the extent these damages are covered by the forms of insurance coverage required above.

g. Evaluation of Adequacy of Coverage

The City of Oakland maintains the right to, acting reasonably, modify, delete, alter or change these requirements, with reasonable notice, upon not less than ninety (90) days prior written notice.

h. Higher Limits of Insurance

If the contractor maintains higher limits than the minimums shown above, the City shall be entitled to coverage for the higher limits maintained by the contractor.

k. *Claims Made Policies*

If any of the required policies provide coverage on a claims-made basis:

1. The Retroactive Date must be shown and must be before the date of the contract or the beginning of contract work.
2. Insurance must be maintained and evidence of insurance must be provided *for at least three (3) years after completion of the contract of work.*
3. If coverage is canceled or non-renewed, and not *replaced with another claims-made policy form with a Retroactive Date* prior to the contract effective date, the Consultant must purchase “extended reporting” coverage for a minimum of *three (3) years* after completion of contract work.

END OF SCHEDULE Q – INSURANCE REQUIREMENT

Attachment F – Oakland Central Square Contract Costing

Application	Software/Services	Qty	One-time Fees	Recurring Renewal/Maintenance			Optional	Optional
				5/1/2022-4/30/2023	5/1/2023-4/30/2024	5/1/2024-4/30/2025	Year 1	Year 2
IQ CrimeView Advanced Reports Annual Subscription Fee	Software	1		\$ 9,975.00	\$ -	\$ -	\$ -	\$ -
IQ - CrimeView Dashboard Annual Subscription Fee	Software	1		\$ 13,615.88	\$ -	\$ -	\$ -	\$ -
IQ CrimeView Desktop License Annual Maintenance Fee	Software	1		\$ 5,622.75	\$ 5,903.89	\$ 6,199.08	\$ 6,509.04	\$ 6,834.49
Crimemapping.com	Software	1		\$ -	\$ -	\$ -	\$ -	\$ -
Quote No. Q-63453								
Professional Services -- Complete P1 integration	Services	N/A	\$ 11,700.00					
CrimeView Analytics: Designer/Admin License Subscription Annual Subscription Fee	Software	4		\$ 3,000.00	\$ 3,150.00	\$ 3,307.50	\$ 3,472.88	\$ 3,646.52
CrimeView Analytics: Single Data Set (3 years data) Non-CST Sys. Subscription - RMS Arrests	Software	1		\$ 2,952.84	\$ 3,100.48	\$ 3,255.51	\$ 3,418.28	\$ 3,589.20
CrimeView Analytics: Single Data Set (3 years data) Non-CST Sys. Subscription - Stop Data (Using field interview data template)	Software	1		\$ 2,952.84	\$ 3,100.48	\$ 3,255.51	\$ 3,418.28	\$ 3,589.20

Attachment F – Oakland Central Square Contract Costing

CrimeView Analytics: Single Data Set (Add'l Yr) Subscription Fee - 7 additional years data- RMS Arrests	Software	7		\$ 3,500.00	\$ 3,675.00	\$ 3,858.75	\$ 4,051.69	\$ 4,254.27
CrimeView Analytics: Single Data Set (Add'l Yr) Subscription Fee - 7 additional years data - Stop Data	Software	7		\$ 3,500.00	\$ 3,675.00	\$ 3,858.75	\$ 4,051.69	\$ 4,254.27
CrimeView Analytics: Standard (3 years data) Non-CST System Subscription - CAD Incident & RMS Incident	Software	1		\$ 7,710.20	\$ 8,095.71	\$ 8,500.50	\$ 8,925.52	\$ 9,371.80
CrimeView Analytics: Standard (Add'l Year) System Subscription - 7 additional years data CAD Incidents & RMS Incidents	Software	7		\$ 4,900.00	\$ 5,145.00	\$ 5,402.25	\$ 5,672.36	\$ 5,955.98
Quote No. Q-62250								
Professional Services	Services	N/A	\$ 5,000.00					

The following Services and Software fees will only be invoiced upon authorization to proceed from the agency. The dates for the Software - Recurring Renewal/Maintenance period are estimated. The actual renewal period will begin on the Go-Live date of the software.

Quote No. Q-64054								
Professional Services -- CrimeView Analytics Upgrade	Services	N/A	\$ 16,380.00					
CrimeView Analytics: Single Data Set (3 years data) Non-CST Sys. Subscription - LPR	Software	1		\$ 1,800.00	\$ 1,890.00	\$ 1,984.50	\$ 2,083.73	\$ 2,187.91

Attachment F – Oakland Central Square Contract Costing

CrimeView Analytics: Single Data Set (3 years data) Non-CST Sys. Subscription - Shotspotter	Software	1		\$ 1,800.00	\$ 1,890.00	\$ 1,984.50	\$ 2,083.73	\$ 2,187.91	
Total			\$ 33,080.00	\$ 61,329.51	\$ 39,625.56	\$ 41,606.84	\$ 43,687.18	\$ 45,871.54	\$ 265,200.6

The prices quantified above are for the software and services contained herein. If any additional software or services are requested, then a change order/amendment shall be entered into with requisite pricing. An increase in the CentralSquare Software licenses granted to the City will result in an increase in the Annual Renewal fees.

City of Oakland Department of Violence Prevention

Surveillance Impact Report: Apricot 360

The Department of Violence Prevention (DVP) was established in 2019 with a mandate to reduce levels of gun violence, intimate partner violence, commercial sexual exploitation, family trauma associated with unsolved homicides, and community trauma associated with ongoing violence in Oakland. The DVP applies a public health approach to violence prevention and intervention efforts that focuses resources on people, neighborhoods, and times of day that are most likely to be impacted by violence. The department also applies different prevention and intervention strategies based on whether individuals are exposed to violence, at risk for violence, or at the center of violence. In Fiscal Year 2022-23, the DVP will distribute \$20 million in funding to community-based organizations in Oakland that deliver prevention and intervention services in the areas of group and gun violence, gender-based violence, and community healing. The DVP also provides direct services in the areas of adult life coaching, violence interruption, and shooting and homicide response. Since 2006, the DVP (formerly Oakland Unite) has collected data on individual- and group-level service delivery, as well as contract management, through the Cityspan data management system. Due to an expanding breadth of services, the DVP and its contracted service providers now require a more sophisticated data management system. The DVP is seeking to contract with Social Solutions Global, Inc. to procure Apricot 360 for this purpose.

A. Description

Social Solutions Global Inc.'s Apricot 360 data management system is the leading cloud software provider for public sector and nonprofit social service organizations. It allows organizations to collect a range of information to facilitate high-quality case management services, and it provides advanced analytics and reporting of collected data through dynamic dashboards. It allows providers to synchronize and manage many programs from the same platform, it allows for easy communication between providers and with clients, and it includes a variety of features that help providers complete their work, such as standardized workflows to ensure key steps are not missed, alerts for missing or incomplete data, mobile data entry capabilities, mechanisms for referring clients to outside agencies, and dashboards that relay organization and client updates to staff in real time. Apricot 360 offers integration capabilities with other data management systems and technology platforms to avoid redundancy in data entry for community-based organizations that use other data management solutions. These are one-way integrations that allow data to enter the Apricot system but do not allow data to be extracted. Apricot 360 also allows organizations to store documents and manage all processes related to contract management, including regular invoicing and tracking of deliverables.

B. Purpose

The purpose of this data management system is for the DVP and its contracted providers to track service delivery methods and outcomes for individuals and groups of individuals engaged in services related to group and gun violence, gender-based violence, and community healing. The data management system will be used by direct service staff to track engagement, milestones, and outcomes for individual clients as well as attendance, duration, and content of group services. Supervisory staff within contracted organizations and within the DVP will use the system to ensure that direct service staff are engaging clients with the expected frequency and delivering services appropriately to facilitate behavior change. The DVP's data and evaluation team will use the data management system to monitor aggregate service

delivery and outcome data across each strategy, track the completion of grantee deliverables, and identify challenges with program implementation that require remediation. The DVP's contract staff will use the system to store contract documents, communicate with grantees about contract questions, track budget spenddown, and receive and process invoices based on completion of deliverables. Finally, service delivery and outcomes data will be available to external evaluators contracted by the DVP to conduct an evaluation of programs and services; these data will be identifiable only if clients have previously signed a consent form agreeing to the release of their identifiable data.

C. Location

Apricot 360 is a cloud-based system that will be accessed via the internet by program staff within the DVP and DVP-funded organizations. Clients served by the data management system will primarily reside in Oakland, CA.

D. Impact

The aggregation of demographic, service delivery, and outcome data on individual clients receiving services through the DVP or DVP-funded organizations in a single data management system poses the following potential risks:

- Data breach: A staff member could accidentally or purposefully download and share client data with unauthorized users, compromising client privacy. Alternatively, a third party could hack into the data management system to access records without authorization.
- Subpoena or public records request: The DVP could be required by law to release individual client records to an outside agency, compromising client privacy.

In a situation where individual data were released to a law enforcement agency, it is possible that the data could be used to support legal allegations regarding an individual being involved in violent activity due to the individual's enrollment in violence prevention or intervention services.

E. Mitigations

The DVP will take special care to ensure that data are only accessed on a need-to-know and right-to-know basis, meaning that staff from the DVP and DVP-funded organizations will only access information within the data management system that is essential to their job function. Apricot 360 allows administrators to restrict staff access to client records and individual fields within client records based on the staff member's pre-determined access requirements. For example, a case manager within a given DVP-funded organization will only have access to service delivery records for clients served by the case manager's organization; the case manager will not have access to service delivery records for clients being served by other organizations. Only staff within the DVP's Data and Evaluation Unit (currently two staff members) will have access to all data across providers (including individual-level client data) to allow for quality assurance reviews and technical assistance. Other administrative staff within the DVP and DVP-funded organizations will only have access to aggregate service delivery data in order to observe overall trends and progress towards meeting contract deliverables.

To prevent against data breaches, either intentional or unintentional, staff within the DVP's Data and Evaluation Unit will extensively train all staff within the DVP and DVP-funded organizations in proper usage of the Apricot 360 system prior to granting access. For more information on this training, please see the DVP's *Surveillance Technology Use Policy*.

In situations when the DVP receives a subpoena or public records request pertaining to data in the Apricot 360 system, the DVP will first consult with the City Attorney’s Office regarding the DVP’s obligation to provide the requested data. If the City Attorney’s Office confirms that data must be provided, the DVP will work closely with the City Attorney’s Office to redact all personally identifiable information (PII) to maintain client privacy. Additionally, clients will be notified in advance of their data being shared in these very rare, unanticipated circumstances.

Hacking attempts will be prevented through strict data security measures that are discussed further under *Data Security* and in **Appendix A**.

The DVP will retain PII on clients engaged in DVP-funded services for three years following service completion to ensure that data are available for impact evaluations conducted by external evaluators, which can last for up to 3 years following service delivery. At the end of three years, PII will be deleted and anonymous service delivery data will be retained for an additional four years to allow the DVP to monitor trends in service delivery over time. At the conclusion of seven years, all data for an individual will be permanently deleted from the Apricot 360 system.

F. Data Types and Sources

Table 1 presents an overview of service delivery and outcome data that will be collected through the data management system. **Table 2** provides an overview of the data management system’s functionality pertaining to contract management, data visualization and extraction, and data management.

Table 1. Service delivery and outcome data collected through the data management system.

Category	Service delivery and outcome data
Individual service delivery	<ul style="list-style-type: none"> ▪ Date, method, and result of outreach attempts ▪ Client name and contact information ▪ Client demographic information (e.g. age, race, gender, education, language spoken at home) ▪ Client’s current education, employment, and housing information ▪ Risk and protective factor assessment results ▪ Program referral, intake, and exit information ▪ Individual flags to identify unique features of clients ▪ Information about important people (contact information and affiliation for family members, spouses, close friends, probation or parole officer, etc.) ▪ Date, duration, and method of all communication involving client (including communication <i>about</i> client with important person or other service provider) ▪ Date, location, type, and duration of all activities involving client ▪ Date, amount, and purpose of financial incentives received ▪ Client outcomes (e.g. obtained GED, completed probation) ▪ Case plan goals, actions, start dates, and completion dates ▪ Date and status of referrals made to other service providers
Group services	<ul style="list-style-type: none"> ▪ Date, location, and duration of service ▪ Number of clients and/or community members engaged ▪ Number of staff members present ▪ Other metrics based on event (e.g. number of meals distributed)

Category	Service delivery and outcome data
Crisis response	<ul style="list-style-type: none"> ▪ Date, time, sender, and recipient of crisis notifications to staff ▪ Date, time, and name of individual responding to the scene or hospital ▪ Victim name and demographics ▪ Incident type (e.g. group/network involved, domestic violence), homicide status, and level of retaliation ▪ Dates, person responsible, and notes on the following categories of response: relocation, mediation, peer outreach, family outreach, and community outreach

Table 2. Data management system functionality pertaining to contract management, data visualization and extraction, and data management.

Category	Functionality requirement
Contract management	<ul style="list-style-type: none"> ▪ Store documents like scope of work, city council resolution, etc. for reference ▪ Display contract budget and show amount remaining in each budget category based on invoices submitted ▪ Allow for invoice submission, approval, and reminders ▪ Allow for communication between DVP staff and CBO staff
Data visualization and extraction	<ul style="list-style-type: none"> ▪ Download raw data in Excel files and customize file downloads to specify fields included, date ranges, etc. ▪ Within the data management system, display easy-to-understand graphs and charts of service or contract data that are relevant to each individual staff member ▪ Customize and generate reports for CBOs or program strategies that present results in comparison to predetermined metrics or deliverables
System and data management	<ul style="list-style-type: none"> ▪ Display or hide specific data fields based on staff credentials ▪ Flag and prompt a correction for missing or incomplete data ▪ Retain historical data entries (e.g. prior program enrollments for clients) ▪ Store consent forms, sign-in sheets, and other scanned documents ▪ Provide mobile database access that allows staff to easily record data in the field (e.g. crime scene response) ▪ Provide a high level of privacy security that complies with the Health Insurance Portability and Accountability Act (HIPAA) ▪ Issue reminders for staff regarding upcoming tasks or inactive clients ▪ Identify and merge duplicate client records ▪ Allow for staff to make service referrals for clients to other providers, both contracted by the DVP and not contracted by the DVP

G. Data Security

The Apricot 360 system has comprehensive measures in place to maintain data privacy and security. Information about Apricot’s security and hosting is attached as **Attachment A**, which states the following: “Social Solutions’ office sits behind a firewall which extensively controls, tracks, and reports access to our internal infrastructure. Our software meets current HUD Domestic Violence, HMIS, and Social Security Administration data management and security protocols, FedRAMP ready, as well as minimum required FERPA and HIPAA standards.” In addition, **Attachment A** states that Apricot 360 uses

“state-of-the art equipment and technology to safeguard the confidential nature of data. Data is automatically encrypted while in transit between your computer and our servers as well as while in the database. Users access Apricot® software web application servers via secure HTTPS connection.”

H. Fiscal Cost

The development of a custom data management system and annual licensing and technical support fees provided by Social Solutions Global Inc. for five years is \$533,056. Funding allocations by fiscal year are outlined in **Table 3**.

Table 3. Budget allocation for Apricot 360 data management system by fiscal year and funding source.

Fiscal year	Description of fees	Funding from Measure Z	Funding from General Purpose Fund or DVP grants	Total amount
2022-2023	Custom system development and implementation	\$70,000	\$1,000	\$71,000
	Annual licenses and training/technical support	\$0	\$49,014	\$49,014
2023-2024	Annual licenses and training/technical support	\$70,000	\$28,028	\$98,028
2024-2025*	Annual licenses and training/technical support	\$70,000	\$28,028	\$98,028
2025-2026*	Annual licenses and training/technical support	\$70,000	\$30,969	\$100,969
2026-2027*	Annual licenses and training/technical support	\$70,000	\$36,017	\$106,017
TBD	Contingency for system development or additional annual licenses	\$0	\$10,000	\$10,000
Total		\$350,000	\$183,056	\$533,056

*Funding allocations in these fiscal years are based on the assumption that Measure Z funding will be reauthorized. If Measure Z is not reauthorized, the DVP will use grant funding or money from the General Purpose Fund to cover the Measure Z allocations.

I. Third Party Dependence

Data collected through Apricot 360 would be stored on Social Solutions Global Inc.’s cloud-based server.

J. Alternatives

One alternative to adopting a contract with Social Solutions Global, Inc. would be to continue using the data management system provided by Cityspan. This would severely limit the DVP’s ability to conduct process and outcome evaluations related to DVP-funded services, and it would limit the system’s utility for direct service staff in supporting service delivery to clients. Functions that are not currently possible in Cityspan are outlined below in **Table 4**.

Table 4. Data management system functions that are not possible using Cityspan.

Category	Function
Individual service delivery	<ul style="list-style-type: none"> ▪ Track outreach efforts with potential clients prior to enrollment, including date, method, and result of each contact ▪ Track multiple program enrollments for a single client ▪ Allow staff to make program or service referrals for clients to outside organizations and track referral acceptance ▪ Flag clients who are inactive and require follow-up ▪ Detect and resolve duplicate client entries ▪ Track client progress on individual life map goals
Crisis response	<ul style="list-style-type: none"> ▪ Automatically notify staff of shooting and homicide incidents that require a response ▪ Track data on deployment, assessment, and response activities ▪ Allow for mobile data entry in the field ▪ Allow for communication within the system between members of the response team to coordinate activities
System and data management	<ul style="list-style-type: none"> ▪ Modify data system fields or functions (done by DVP staff) ▪ Download raw service delivery data at the client level rather than the provider level for internal analysis ▪ Flag and prompt the correction of missing or incomplete data ▪ Present up-to-date data to DVP staff and grantees through visually-appealing dashboards ▪ Allow for automated communication between other grantee data management systems & the DVP's data management system ▪ Allow for staff to make service referrals for clients to other providers, both contracted by the DVP and not contracted by the DVP

Another alternative to adopting a contract with Social Solutions Global, Inc. would be to select a different vendor to develop a new data management system for the DVP and provide ongoing user licenses, hosting, and technical assistance. **Table 5** provides cost information from two comparison quotes that the DVP solicited from Salesforce and Microsoft Corporation pertaining to the requested data management services.

Table 5. Proposal costs from three vendors that meet the DVP's data management system requirements.

Vendor	Location of company headquarters	Average annual license and technical assistance cost	One-time development cost	Contingency cost	Total contract amount
Social Solutions	Austin, Texas	\$90,411	\$71,000	\$10,000	\$533,056
Salesforce	San Francisco, California	\$58,548	\$173,700	\$10,000	\$476,440
Microsoft Corporation	Redmond, Washington	\$9,300	\$1,053,000	\$10,000	\$1,099,500

As demonstrated in Table 5, the proposal from Social Solutions is \$56,616 greater than the proposal from Salesforce, which equates to \$11,323 per year. However, the maintenance and administration of a Salesforce system requires very specialized training that would likely require the DVP to hire an additional staff person or contract with a Salesforce consultant on an ongoing basis, which would significantly increase the annual costs. After reviewing demonstrations of both the Social Solutions and Salesforce systems, DVP staff felt strongly that the Apricot 360 system was significantly less complex and easier to use. Additionally, Social Solutions specializes in local government, non-profits, and social services, while Salesforce does not. The proposal submitted by Microsoft Corporation was excessive in terms of cost and therefore not considered a viable alternative.

K. Track Record

Social Solutions Global Inc. already contracts with a number of similar social service agencies, including the Oakland Unified School District, the City of Stockton's Office of Violence Prevention, the City of Los Angeles Mayor's Office of Gang Reduction and Youth Development (GRYD), Roca, Inc. (a nationally-renowned violence intervention agency located in Boston, MA), and five organizations currently funded by the DVP. Social Solutions also received a strong endorsement from Empower Tehama, a service provider based in Northern California that provides services similar to the DVP, during a reference check conducted by DVP staff.

Additionally, Social Solutions Global, Inc. estimates that the implementation of their data management system saves approximately 35% time on data entry, 75% time on reporting, and 25% time on reconciling data integrity issues.

apricot[®] Security and Hosting

Social Solutions Global, Inc. ("SSG") takes comprehensive measures to ensure that data is kept safe, confidential and recoverable in the case of a disaster. Social Solutions' office sits behind a firewall which extensively controls, tracks, and reports access to our internal infrastructure. Our software meets current **HUD Domestic Violence**, **HMIS**, and **Social Security Administration** data management and security protocols, **FedRAMP** ready, as well as minimum required **FERPA** and **HIPAA** standards.

Data Security

Apricot[®] uses user names and passwords to prevent unauthorized access and to restrict user access within the application. Each unique user account is assigned access to programs and permission sets to restrict access to data and features in the system. Customer data is housed in two locations (U.S. and Canada) based on the location of the client. Data is stored using redundant AWS hardware technologies, SSG fault tolerant software, and journaling file systems.

PASSWORDS

- ✓ can be set to have a minimum length
- ✓ can be set to contain non-alpha-numeric characters
- ✓ can be set to expire
- ✓ can be locked after a set # of invalid login attempts
- ✓ can be changed by a local administrator
- ✓ are not displayed upon entry and are encrypted

Encryption

Social Solutions uses state-of-the-art equipment and technology to safeguard the confidential nature of your data. Your data is automatically encrypted while in transit between your computer and our servers as well as while in the database. Users access Apricot[®] software web application servers via secure HTTPS connection.

SOC2

Our SOC2 Type 2 (SSAE18) report is a comprehensive document that describes Social Solutions security controls in the domains of Administrative, Physical, and Technical security. Apricot is certified SOC 2 Type II compliant. SSG security controls are reviewed by independent external auditors during audits for our SOC compliance.

Amazon Web Services (AWS) Server Security

Each of our servers is individually governed by a system that is designed to prevent unexpected Internet data from being processed by our server software. IDS, virus scanning, automated system checks, and remote logging guard against unauthorized access. AWS implements electronic surveillance and multi-factor access control systems to secure its data centers. Data centers are staffed 24x7 by trained security guards, and access must be strictly authorized. Multiple availability zones allow Apricot to remain resilient in the face of most failure modes, including natural disasters or system failures¹. In case of a disaster in our main AWS region, Social Solutions will have Apricot up and running between 24-48 hours in a backup AWS region.

REDUNDANT INFRASTRUCTURE AND BACKUPS

- ✓ 24/7/365 monitoring of uptime across the infrastructure
- ✓ Redundant water, power, telecommunications, and Internet connectivity to maintain continuous operations
- ✓ Uninterrupted power supply to reduce possible service outages

RETENTION POLICY

- ✓ Keep daily backups for 12 months

Compliance

The AWS cloud infrastructure has been designed and managed by Amazon.com². AWS adheres to:

- ✓ SOC 1/SSAE 16/ISAE 3402 (formerly SAS70)
- ✓ SOC 2
- ✓ SOC 3
- ✓ PCI DSS Level 1
- ✓ ISO 270012

¹ For additional information visit: https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

² For additional information visit: https://d0.awsstatic.com/whitepapers/compliance/AWS_Compliance_Quick_Reference.pdf

City of Oakland Department of Violence Prevention

Surveillance Technology Use Policy: Apricot 360

The Department of Violence Prevention (DVP) was established in 2019 with a mandate to reduce levels of gun violence, intimate partner violence, commercial sexual exploitation, family trauma associated with unsolved homicides, and community trauma associated with ongoing violence in Oakland. The DVP applies a public health approach to violence prevention and intervention efforts that focuses resources on people, neighborhoods, and times of day that are most likely to be impacted by violence. The department also applies different prevention and intervention strategies based on whether individuals are exposed to violence, at risk for violence, or at the center of violence. In Fiscal Year 2022-23, the DVP will distribute \$20 million in funding to community-based organizations in Oakland that deliver prevention and intervention services in the areas of group and gun violence, gender-based violence, and community healing. The DVP also provides direct services in the areas of adult life coaching, violence interruption, and shooting and homicide response.

A. Purpose

The purpose of the Apricot 360 data management system, developed by Social Solutions Global, Inc., is for the DVP and its contracted providers to track service delivery methods and outcomes for individuals and groups of individuals engaged in services related to group and gun violence, gender-based violence, and community healing, as well as to manage contracts between the DVP and funded organizations. The data management system will be used by direct service staff to track engagement, milestones, and outcomes for individual clients as well as attendance, duration, and content of group services. Supervisory staff within contracted organizations and within the DVP will use the system to ensure that direct service staff are engaging clients with the expected frequency and delivering services appropriately to facilitate behavior change. Staff within the DVP's Data and Evaluation Unit will use the data management system to monitor aggregate service delivery and outcome data across each strategy, track the completion of grantee deliverables, and identify challenges with program implementation that require remediation. The DVP's contract staff will use the system to store contract documents, communicate with grantees about contract questions, track budget spenddown, and receive and process invoices based on completion of deliverables. Finally, service delivery and outcomes data will be available to external evaluators contracted by the DVP to conduct an evaluation of programs and services; these data will be identifiable only if clients have previously signed a consent form agreeing to the release of their identifiable data.

B. Authorized Use

All data will be accessed on a need-to-know and right-to-know basis, meaning that individuals will only be able to access information within the data management system that is essential to their job function. Categories of data management system usage are described below.

- **Service delivery:** Direct service staff and supervision staff will use the data management system to track information on client contacts, progress towards milestones, accomplishments, referrals, and other aspects of service delivery. The system will track tasks related to service delivery and present summarized data on clients served through dashboards that are helpful to staff who are directly responsible for service delivery to clients.

- **Contract management:** DVP program officers will use aggregate data entered into the data management system to ensure that providers are delivering services as outlined in their scopes of work and meeting contract deliverables. Program officers will also use the system to manage grant budgets, budget and scope modifications, invoicing and payments, and communication with grantees about contracts.
- **Internal evaluation:** DVP staff in the Data and Evaluation Unit will use data from the system to ensure that the department is serving the correct target population, that services are being delivered as expected, and that summarized service delivery data are available to a range of external stakeholders, including councilmembers, committee members, grantors, and the public.
- **External evaluation:** External evaluators contracted by the DVP or City Administrator’s Office will use the data from the data management system to evaluate the effectiveness of services delivered by the DVP or DVP-funded agencies. Evaluators will seek and receive Institutional Review Board (IRB) approval prior to commencing any research activities. Once IRB approval is obtained, evaluators will only have access to personally identifiable information (PII) of individuals who sign a consent form agreeing to have their data be shared with a third-party evaluator. For clients who do not sign a consent form, data from the data management system will only be provided without PII or in aggregate form.

C. Data Collection

Data will be collected by direct service staff with the DVP and DVP-funded agencies. Prior to enrollment in services, individuals will complete consent forms pertaining to general storage of their information in the data management system and, separately, potential use of their data by a third-party evaluator. Direct service staff will then enter in data provided by participants or related to participant interactions with the staff member into the data management system in accordance with the signed consent forms.

Table 1 presents an overview of service delivery and outcome data that will be collected through the data management system. **Table 2** provides an overview of the data management system’s functionality pertaining to contract management, data visualization and extraction, and data management.

Table 1. Service delivery and outcome data collected through the data management system.

Category	Service delivery and outcome data
Individual service delivery	<ul style="list-style-type: none"> ▪ Date, method, and result of outreach attempts ▪ Client name and contact information ▪ Client demographic information (e.g. age, race, gender, education, language spoken at home) ▪ Client’s current education, employment, and housing information ▪ Risk and protective factor assessment results ▪ Program referral, intake, and exit information ▪ Individual flags to identify unique features of clients ▪ Information about important people (contact information and affiliation for family members, spouses, close friends, probation or parole officer, etc.)

Category	Service delivery and outcome data
	<ul style="list-style-type: none"> ▪ Date, duration, and method of all communication involving client (including communication <i>about</i> client with important person or other service provider) ▪ Date, location, type, and duration of all activities involving client ▪ Date, amount, and purpose of financial incentives received ▪ Client outcomes (e.g. obtained GED, completed probation) ▪ Case plan goals, actions, start dates, and completion dates ▪ Date and status of referrals made to other service providers
Group services	<ul style="list-style-type: none"> ▪ Date, location, and duration of service ▪ Number of clients and/or community members engaged ▪ Number of staff members present ▪ Other metrics based on event (e.g. number of meals distributed)
Crisis response	<ul style="list-style-type: none"> ▪ Date, time, sender, and recipient of crisis notifications to staff ▪ Date, time, and name of individual responding to the scene or hospital ▪ Victim name and demographics ▪ Incident type (e.g. group/network involved, domestic violence), homicide status, and level of retaliation ▪ Dates, person responsible, and notes on the following categories of response: relocation, mediation, peer outreach, family outreach, and community outreach

Table 2. Data management system functionality pertaining to contract management, data visualization and extraction, and data management.

Category	Functionality requirement
Contract management	<ul style="list-style-type: none"> ▪ Store documents like scope of work, city council resolution, etc. for reference ▪ Display contract budget and show amount remaining in each budget category based on invoices submitted ▪ Allow for invoice submission, approval, and reminders ▪ Allow for communication between DVP staff and CBO staff
Data visualization and extraction	<ul style="list-style-type: none"> ▪ Download raw data in Excel files and customize file downloads to specify fields included, date ranges, etc. ▪ Within the data management system, display easy-to-understand graphs and charts of service or contract data that are relevant to each individual staff member ▪ Customize and generate reports for CBOs or program strategies that present results in comparison to predetermined metrics or deliverables
System and data management	<ul style="list-style-type: none"> ▪ Display or hide specific data fields based on staff credentials ▪ Flag and prompt a correction for missing or incomplete data ▪ Retain historical data entries (e.g. prior program enrollments for clients) ▪ Store consent forms, sign-in sheets, and other scanned documents ▪ Provide mobile database access that allows staff to easily record data in the field (e.g. crime scene response) ▪ Provide a high level of privacy security that complies with the Health Insurance Portability and Accountability Act (HIPAA) ▪ Issue reminders for staff regarding upcoming tasks or inactive clients

Category	Functionality requirement
	<ul style="list-style-type: none"> <li data-bbox="451 239 1024 268">▪ Identify and merge duplicate client records <li data-bbox="451 275 1398 327">▪ Allow for staff to make service referrals for clients to other providers, both contracted by the DVP and not contracted by the DVP

D. Data Access

The DVP will take special care to ensure that data are only accessed on a need-to-know and right-to-know basis, meaning that staff will only be able to access information within Apricot 360 that is essential to their job function. Apricot 360 allows administrators to restrict access to client records and individual fields within client records for staff members based on their pre-determined access requirements. For example, a case manager within a given DVP-funded organization will only have access to service delivery records for clients served by the case manager’s organization; the case manager will not have access to service delivery records for clients being served by other organizations. Only staff within the DVP’s Data and Evaluation Unit (currently two staff members) will have access to all data across providers (including individual-level client data) to allow for quality assurance reviews and technical assistance. Other administrative staff within the DVP and DVP-funded organizations will only have access to aggregate service delivery data in order to observe overall trends and progress towards meeting contract deliverables. Unauthorized use of the system by any staff person with any level of access will lead to disciplinary action, which could include termination of a service provider’s grant agreement and cessation of funding and, with respect to City employees, discipline up to and including termination.

E. Data Protection

The Apricot 360 system has comprehensive measures in place to maintain data privacy and security. Information about Apricot’s security and hosting is attached as **Attachment A**, which states the following: “Social Solutions’ office sits behind a firewall which extensively controls, tracks, and reports access to our internal infrastructure. Our software meets current HUD Domestic Violence, HMIS, and Social Security Administration data management and security protocols, as well as minimum required FERPA and HIPAA standards.” In addition, Attachment A states that Apricot 360 uses “state-of-the art equipment and technology to safeguard the confidential nature of data. Data is automatically encrypted while in transit between your computer and our servers as well as while in the database. Users access Apricot® software web application servers via secure HTTPS connection.”

F. Data Retention

The DVP will retain PII on clients engaged in DVP-funded services for three years following service completion to ensure that data are available for evaluations conducted by external evaluators, which can last for up to 3 years following service delivery. At the end of three years, PII will be deleted and anonymous service delivery data will be retained for an additional four years to allow the DVP to monitor trends in service delivery over time. At the conclusion of seven years, all data for an individual will be permanently deleted from the Apricot 360 system.

G. Public Access

There will be absolutely no public access to raw data in this system. As with any government record, a member of the public may submit a Public Records Act Request, but only aggregate data with no PII would be released subject to any applicable federal, state, and local privacy and/or confidentiality laws.

Aggregated data from this system (e.g. how many individuals were served in a specific strategy during a specific year) will be available in the evaluation reports and may be available in tables, charts, or dashboards in public documents or through the DVP's public website.

H. Third Party Data Sharing

No other city departments will have access to this data. An external evaluator contracted by the DVP or the City Administrator's Office will use the data in this system for evaluation purposes to examine the effectiveness of programs. They will only have access to the individual-level data for individuals who sign a consent form allowing their data to be shared with a third-party evaluator. For clients who do not sign a consent form, data will only be provided to a third-party evaluator without individual identifiers or in aggregate form.

I. Training

Staff within the DVP's Data and Evaluation Unit will attend the Apricot 360 Train-the-Trainer and Custom End User training sessions, which will review the data management system's configuration and review tips and tricks for training end users. In addition, DVP staff will have access to the Apricot Basic Training package, which includes unlimited access to the following:

- Live Apricot Setup Webinar
- Live Apricot Insights Webinar
- Administrative Video Library
- End User Training Library

Using these tools, staff within the DVP's Data and Evaluation Unit will train internal DVP staff and staff from DVP-funded organizations on how to use the new data system. This will include general trainings, trainings specific to staff members' strategy and sub-strategy areas, and ongoing options for one-on-one training, support, and technical assistance. All trainings will specify appropriate usage of the system pertaining to data privacy and consequences of inappropriate system usage, which could include termination of a service provider's grant agreement and cessation of funding and, with respect to City employees, discipline up to and including termination.

J. Auditing and Oversight

The DVP's Budget and Grants Administrator will be responsible for ensuring that the Surveillance Use Policy is followed by internal DVP staff and staff from DVP-funded organizations. All actions in the system (add, edit, delete, view, etc.) are accessible through audit log reporting built into the system for administrator monitoring. The DVP's Budget and Grants Administrator will review audit logs on a monthly basis to ensure appropriate system usage by all users. Any indication of inappropriate system usage will be thoroughly investigated by the DVP in consultation with the City Attorney's Office. Inappropriate system usage could result in termination of a service provider's grant agreement and cessation of funding and, with respect to City employees, discipline up to and including termination.

K. Maintenance

Social Solutions Global Inc.'s security mechanisms and procedures are built on the Soc2 Type II Framework with HIPAA amendment and audited by third-party security experts annually for meeting best-in-class technical safeguards, processes, policies, and procedures. Social Solutions Global Inc. has an extensive cloud security team led by their Chief Information Security Officer that uses a broad set of tools for monitoring security, vulnerability, integrity, uptime, and more across over 19,000 customers. A complete copy of Social Solutions Global Inc.'s Soc2 Type II has been shared with City of Oakland staff who have signed a non-disclosure agreement, including staff from the DVP's Data and Evaluation Unit and the Information Technology Department.

apricot[®] Security and Hosting

Social Solutions Global, Inc. ("SSG") takes comprehensive measures to ensure that data is kept safe, confidential and recoverable in the case of a disaster. Social Solutions' office sits behind a firewall which extensively controls, tracks, and reports access to our internal infrastructure. Our software meets current **HUD Domestic Violence**, **HMIS**, and **Social Security Administration** data management and security protocols, **FedRAMP** ready, as well as minimum required **FERPA** and **HIPAA** standards.

Data Security

Apricot[®] uses user names and passwords to prevent unauthorized access and to restrict user access within the application. Each unique user account is assigned access to programs and permission sets to restrict access to data and features in the system. Customer data is housed in two locations (U.S. and Canada) based on the location of the client. Data is stored using redundant AWS hardware technologies, SSG fault tolerant software, and journaling file systems.

PASSWORDS

- ✓ can be set to have a minimum length
- ✓ can be set to contain non-alpha-numeric characters
- ✓ can be set to expire
- ✓ can be locked after a set # of invalid login attempts
- ✓ can be changed by a local administrator
- ✓ are not displayed upon entry and are encrypted

Encryption

Social Solutions uses state-of-the-art equipment and technology to safeguard the confidential nature of your data. Your data is automatically encrypted while in transit between your computer and our servers as well as while in the database. Users access Apricot[®] software web application servers via secure HTTPS connection.

SOC2

Our SOC2 Type 2 (SSAE18) report is a comprehensive document that describes Social Solutions security controls in the domains of Administrative, Physical, and Technical security. Apricot is certified SOC 2 Type II compliant. SSG security controls are reviewed by independent external auditors during audits for our SOC compliance.

Amazon Web Services (AWS) Server Security

Each of our servers is individually governed by a system that is designed to prevent unexpected Internet data from being processed by our server software. IDS, virus scanning, automated system checks, and remote logging guard against unauthorized access. AWS implements electronic surveillance and multi-factor access control systems to secure its data centers. Data centers are staffed 24x7 by trained security guards, and access must be strictly authorized. Multiple availability zones allow Apricot to remain resilient in the face of most failure modes, including natural disasters or system failures¹. In case of a disaster in our main AWS region, Social Solutions will have Apricot up and running between 24-48 hours in a backup AWS region.

REDUNDANT INFRASTRUCTURE AND BACKUPS

- ✓ 24/7/365 monitoring of uptime across the infrastructure
- ✓ Redundant water, power, telecommunications, and Internet connectivity to maintain continuous operations
- ✓ Uninterrupted power supply to reduce possible service outages

RETENTION POLICY

- ✓ Keep daily backups for 12 months

Compliance

The AWS cloud infrastructure has been designed and managed by Amazon.com². AWS adheres to:

- ✓ SOC 1/SSAE 16/ISAE 3402 (formerly SAS70)
- ✓ SOC 2
- ✓ SOC 3
- ✓ PCI DSS Level 1
- ✓ ISO 270012

¹ For additional information visit: https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

² For additional information visit: https://d0.awsstatic.com/whitepapers/compliance/AWS_Compliance_Quick_Reference.pdf



MEMORANDUM

TO: LeRonne L. Armstrong
Chief of Police

FROM: Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

SUBJECT: Automated License Plate Reader –
2021 Annual Report

DATE: March 22, 2022

Background

Oakland Police Department (OPD) ALPR Policy 430 (430.8 Agency Monitoring and Controls) states that the “ALPR Coordinator shall provide the Chief of Police and Public Safety Committee with an annual report for the previous 12-month period.” Policy 430 precedes City Council adoption of the Surveillance Technology Ordinance, enshrined in Oakland Municipal Code (OMC) 9.64; OMC 9.64 separately also requires annual reports as well as review and recommendation of a Surveillance Use Policy (SUP) and Surveillance Impact Report (SIR) – referred to collectively as “Privacy Policy.”

The following bullet points outline the history of OPD’s presentation of ALPR Privacy Policy documents to the City’s Privacy Advisory Commission (PAC):

- January 2019 - Presentation of draft ALPR Privacy Policy.
- February 2019 - Presentation of draft ALPR Privacy Policy.
- April 2019 - Presentation of draft ALPR Privacy.
- January 2021 - Presentation of revised ALPR Privacy Policy and 2019 / 2020 Annual Reports.
- February 2021 - Presentation of revised ALPR Privacy Policy; PAC vote to recommend to the City Council that OPD be prohibited from using ALPR technology for two years.
- OPD then presented the ALPR Privacy Policy and 2019 / 2020 Annual Reports to the Public Safety Committee on May 11, and City Council on May 18. The City Council was presented with two options – OPD’s recommendation to approve the privacy policy as well as the PAC recommendation. The full City Council voted to send the Policy back to the PAC for further review and that OPD provide all missing information.
- August 2021 - Presentation of revised ALPR Privacy Policy and 2019 / 2020 Annual Reports.
- October 2021- Presentation of revised ALPR Privacy Policy and 2019 / 2020 Annual Reports; PAC commissioners suggest having an ad-hoc meeting but then confirm that there are not enough commissioners who are prepared to hold an ad-hoc meeting.
- November 2021- Presentation of revised ALPR Privacy Policy and 2019 / 2020 Annual Reports – at this meeting the PAC again votes to recommend a two-year moratorium OPD use of ALPR technology.

OPD is preparing to again present its Privacy Policy to the City’s Public Safety Committee along with the PAC November 2021 motion for a two-year moratorium at the time of the production of this report.

2021 Annual Report Details

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

Table 1 below shows the total scans and hits by month – the total license plate photographs made and stored each month (1,980,132 scans total for the year). Table 1 also shows the number of times the vehicle-based systems had a match (“hit”) with a California Department of Justice (CA DOJ) database (2,503 total for 2021). OPD’s very outdated ALPR system can only quantify these two figures; the system can no longer quantify individual queries or perform any audit functions, as the software is no longer supported from the original vendor. Prior, the system could run reports that detailed the reasons for queries (e.g. a type of criminal investigation). OPD can only provide more comprehensive use data if and when a newer ALPR system is acquired.

Table 1: 2021 OPD ALPR Scans and Hits

Month	Year	Scans	Hits
Jan	2021	198,027	235
Feb	2021	145,547	229
Mar	2021	212,367	238
Apr	2021	166,993	146
May	2021	184,147	235
Jun	2021	155,502	135
Jul	2021	98,814	110
Aug	2021	190,136	249
Sep	2021	221,509	375
Oct	2021	161,789	242
Nov	2021	121,565	143
Dec	2021	123,736	166
2021 Totals		1,980,132	2503

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

The Federal Bureau of Investigation (FBI) had access to OPD ALPR data without following the standard data access request protocols outlined in Policy 430.9 “Releasing or Sharing ALPR Data,” OPD has provided this level of access because there is a Council-approved Safe Streets Task Force Memorandum of Understanding (MOU)¹. OPD believes that the Task Force MOU allowed for ALPR data-sharing with specific FBI agents who have been co-located with OPD in the Police Administration Building and worked on homicide cases. However, OPD personnel ran an audit of ALPR data queries and discovered that there were

¹ The mission of the FBI San Francisco Violent Crimes Safe Streets Task Force MOU is to identify and target for prosecution criminal enterprise groups and individual responsible for crimes of violence such as murder and aggravated assault, as well as other serious crimes. The MOU does not specifically address the sharing of ALPR data; however, the MOU does specifically articulate protocols for data sharing.

no queries from these FBI personnel. OPD has decided to revoke access to FBI these agents as of 9/28/2021 to alleviate concerns over data privacy.

OPD has not received requests for ALPR data in 2021 from outside police agencies.

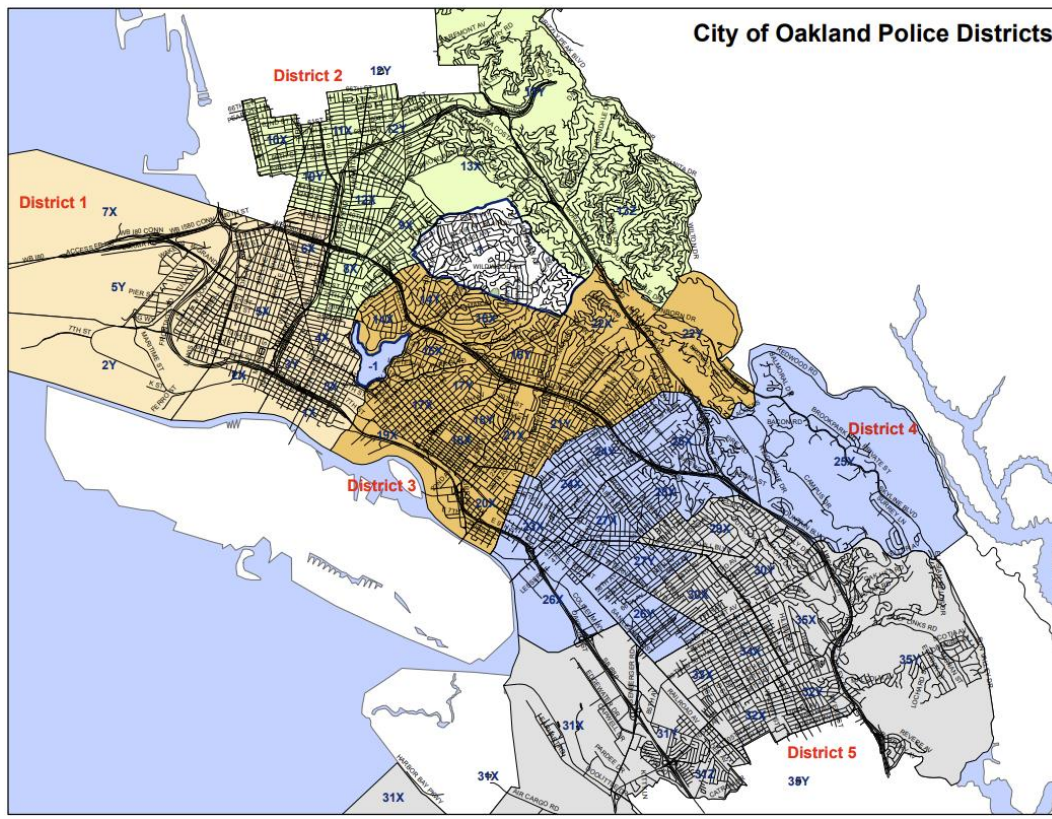
- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The ALPR cameras are installed upon fully marked OPD patrol vehicles (24 operational; 8 inoperable).

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

These vehicles are assigned to the Bureau of Field Operations I (administered out of the Police Administration Building in downtown Oakland) as well as Bureau of Field Operations II (administered from the Eastmont Substation). The vehicles are deployed throughout the City in a patrol function to allow for large areas of the City to have ALPR coverage as the patrol vehicles are used to respond to calls for police service; Figure 1 below is a map showing where patrol vehicles equipped with ALPR are generally deployed throughout the City.

Figure 1: ALPR-Equipped Patrol Vehicle Deployment Distribution



- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Members of the public have spoken at PAC meetings regarding concerns of negative impacts to privacy protections (e.g., that OPD could use ALPR server data to establish travel patterns of particular vehicles associated with particular license plates, and/or that ALPR data can be inadvertently released through inadequate privacy protocols). OPD has also heard comments that more advanced ALPR systems may be used to track other vehicle attributes (e.g., bumper stickers). More recently, OPD staff have also heard from members of the public in support of ALPR systems and wanting to be sure that OPD utilizes technology appropriately to support OPD investigations. Furthermore, OPD personnel are of media reports of ALPR systems where a lack of updates between local systems and State CA DOJ databases lead to inaccurate stolen vehicle notifications, which have led law enforcement to stopping motorists because of stolen vehicle notifications.

OPD is not able to provide the race of each person connected to each ALPR scan. Race data is not captured in the scan itself as explained in the ALPR Draft Surveillance Impact Report. Race data would only be captured if there is a related criminal investigation for a particular ALPR scan capture. Staff could attempt to connect each scan to the associated vehicle registration of each scanned license plate. However, staff would not know if the vehicle driver, at the time of the ALPR scan, is the same person as the registered owner of the vehicle. Furthermore, staff believes that the potential for greater invasiveness in capturing this data outweighs the public benefit of capturing the data. Staff therefore recommend that the PAC makes the determination, that the administrative burden in collecting or verifying this information as well as the associated potential for greater invasiveness in capturing such data outweighs the public benefit.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

The current system is outdated, and the software is not supported from the original vendor. Prior to this loss in function, the system could be used to run reports for sample audits that detailed the reasons for queries (e.g., type of criminal investigation). The ALPR system can currently quantify only hit and scan data as noted in Part A above. OPD currently faces a “Catch-22” situation: OPD cannot produce audits and annual reports that meet the expectations of the Surveillance Technology Ordinance because its current ALPR database and software are outdated and only partially functional. OPD can update the system for approximately \$16,000 – but pursuant to the surveillance ordinance, OPD cannot update the system unless the City Council first approves OPD’s ALPR Use Policy. The PAC has cited OPD’s failure to produce audits and annual reports as a significant reason for the PAC’s refusal to support OPD’s Use Policy and its continued use of ALPR. Staff wants to comply with all facets of the City’s Surveillance Ordinance (OMC 9.64) and continue to bring annual reports to the PAC for ongoing independent oversight of this useful technology, but it cannot do so unless it upgrades its ALPR technology.

OPD created a new ALPR Training document in 2020; OPD staff audited the OPD online training and document review system to ensure that staff completed the ALPR Training module. Approximately 75% of staff have completed the training thus far and OPD is implementing directives to ensure 100% compliance.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

The City’s Information Technology Department (ITD) confirmed to OPD that they have not detected any ALPR information breaches at the time of OPD’s inquiry for the production of this annual report.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Table 2 below provides 2021 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2021 year

Table 2: 2021 OPD Type 1 Crime Data

Part 1 Crimes <i>All totals include attempts except homicides</i>	01-01-2020 through 12-31-2020	01-01-2021 through 12-31-2021	Year-to-Date % Change 2020 vs. 2021	3-Year Year-to-Date Average	YTD 2021 vs. 3-Year YTD Average
Homicide - 187(a)	102	124	22%	100	24%
• Homicide - all other *	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• With Firearm	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• Auto	6,221	8,179	31%	8,921	-8%
• Residential	1,247	1,055	-15%	1,370	-23%
• Commercial	958	670	-30%	750	-11%
• Other/Unknown	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

Additionally, ALPR was used to recover 39 stolen vehicles recovered with a value an estimated value of \$227,337. **Appendix A** to this report provides additional information about stolen vehicles and/or vehicles involved in carjackings where ALPR played a notification and/or investigatory role.

- I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

OPD has received two new PRRs in 2021 related to ALPR; there were five total open ALPR-related PRRs as of December 31, 2021.

These requests related to the number of ALPR camera systems (see Section C above), ALPR data (the license plate number, date, time, and location information for each license plate recorded for related to either specific license plates or all captured data during certain time periods), and OPD emails related to ALPR data. Other requests related to the sharing of data with other agencies as outlined in Section B above. There are also PRRs relating to technology contracts.

For all ALPR PRRs, OPD can generally provide date and time information. OPD cannot provide information related to locations where license plates were photographed, nor information related to the specific vehicles. Some of these PRRs have been processed and

completed in 2022 during the time of the production of this report – status information below reflects recent updates made in 2022.

No.#	PRR#	Nature of Request	Status	Content Provided
1	RT 16630	All records responsive to the below requests dated from January 1, 2014 through July 28, 2016. - The full documentation of all contracts or non-disclosure agreements (enacted OR IN EFFECT between the above dates) with the companies "Persistent Surveillance Systems" or "Vigilant Solutions" (more of request: https://oaklandca.nextrequest.com/requests/RT-16630).	Still being processed	n/a
2	18-649 –	The names of all agencies, organizations and entities with which the Oakland Police department shares Automatic License Plate Reader ("ALPR") data, such as the National Vehicle Location Service; * The names of all agencies and organizations from which the department receives ALPR data; * The names of all agencies and organizations from which the department shares "hot list" information; * The names of all agencies and organizations from which the department receives "hot list" information; more of request: https://oaklandca.nextrequest.com/requests/18-649	open	OPD ALPR Policy 430: https://oaklandca.nextrequest.com/documents/618507/download
3	19-1546	How many automated license plate readers the Oakland Police Department has in use currently? Are they in fixed locations or on police cars, or other? How many vehicles on your hotlist currently? What's is the hit rate currently, and what was it in March 2018? How long is this data retained for? Is there a formal data retention limit? Have you shared any of this LPR data with any third parties, including non law enforcement bodies? If so, who? Have you bought license plate data from any third parties, and if so who? Has there been any communication between the department and representatives from	Open	Content not yet provided

No.#	PRR#	Nature of Request	Status	Content Provided
		<i>or people acting on behalf of US Immigration and Customs enforcement and / or US Border Patrol? If so, please can you share all correspondence (inc attachments)? More information: https://oaklandca.nextrequest.com/requests/19-1546</i>		
4	21-6410	<i>Requesting ALPR Data for the last two years</i>	<i>open</i>	
5	21-6660	<i>Please provide me with an electronic copy (preferably PDF) of the guidelines and procedures referenced here in OPD's ALPR policy 430 enacted in 2016, including all amendments and revisions thereto: "The Bureau of Services Deputy Chief shall be the administrator of ALPR program, and shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq." Please provide records from the years 2016-2021.</i>	<i>open</i>	

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Zero; OPD did not incur any maintenance, licensing, or training costs. Training is completed using OPD's online portal as well as staff time.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

OPD and the PAC are developing and reviewing a new ALPR Surveillance Policy contemporaneous to the production of this report for OPD ALPR Use Policy 430. OPD is requesting PAC review and recommendation to City Council of this new Surveillance Use Policy (SUP). This new policy will cover all required areas of OMC 9.64.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

LeRonne L. Armstrong,
Chief of Police

Reviewed by,
Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Carlo Beckman, Police Services Manager
OPD, Research and Planning Section

Prepared by:
Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Section

David Pullen, Officer
OPD, IT Unit, Bureau of Services

Appendix A

ALPR Stolen or Carjacked Vehicle Data 2021

For all the examples below, officers performed necessary verification of the stolen vehicle status before acting.

1. 21-001682; 01/11/2021 – Officers on patrol had an ALPR hit on the 1600 block of 18th Street. The vehicle was unoccupied and reported carjacked by San Francisco PD. Vehicle was recovered and towed per SFPD's request. Age of data: ~6days
 - a. Vehicle Data: 2005 Ford F-150
2. 21-001802; 01/11/2021– Officers on patrol had an ALPR hit on the 200 block of 19th Street. The vehicle was unoccupied and reported stolen by South San Francisco PD. Vehicle was recovered and towed per SSFPD's request. Age of data: ~2 days.
 - a. Vehicle Data: 2000 Chevy Tahoe
3. 21-002447; 02/09/2021 – Officers on patrol had an ALPR hit on the 1100 block of E. 15th Street. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~26 days.
 - a. Vehicle Data: 1990 Mazda 626 DX/LX
4. 20-056291; 01/17/2021 – Officers on patrol had an ALPR hit on the 1600 block of 8th Street. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~14 months.
 - a. Vehicle Data: 2000 Ford Focus
5. 21-002722; 01/18/2021 – Officers on patrol had an ALPR hit on the 1300 block of 5th Street. The vehicle was occupied, and officers attempted to detain the suspects, who fled. The vehicle was reported stolen by Berkeley PD. Age of data: ~2 days
 - a. Vehicle Data: 2016 Mazda CX5
6. 21-003887; 01/26/2021 – Officers on patrol had an ALPR hit on the 9700 block of B Street. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~7 days.
 - a. Vehicle Data: 2000 Honda CRV
7. 21-006106; 03/15/2021 – Officers on patrol had an ALPR hit in the area of Fruitvale Ave & Foothill Blvd. The vehicle was occupied, and a stop was conducted. The driver was the registered owner of the vehicle and did not update OPD when they found and recovered the vehicle on 02/08/2021. The driver/registered owner was released. Vehicle was associated with strong-arm robbery, assault & battery, and kidnapping (initially of the victim). Age of data: ~1 month.
 - a. Vehicle Data: 2003 Nissan Maxima
8. 21-006112; 02/08/2021 – Officers on patrol had an ALPR hit on the 3800 block of San Leandro Street. The vehicle was reported stolen out of San Leandro PD. The vehicle was unoccupied, and the vehicle was recovered and towed. Age of data: ~10 days.
 - a. Vehicle Data: 1998 Nissan Frontier

9. 21-006743; 02/17/2021 – Officers on patrol had an ALPR hit on the 250 block of 7th Street. The vehicle was unoccupied, attempts to contact the owner were successful, and the vehicle was released to them. Age of data: ~6 days.
 - a. Vehicle Data: 1999 Ford F-150
10. 21-009814; 03/05/2021 – Officers on patrol had an ALPR hit on the 2800 block of 14th Avenue. The vehicle was unoccupied, attempts to contact the owner were successful, and the vehicle was released to a friend of the owner. Age of data: ~3 days.
 - a. Vehicle Data: 1991 Honda Civic
11. 21-010933; 03/09/2021 – Officers on patrol had an ALPR hit on the 600 block of 6th Street. The vehicle was occupied, and the individual was detained and arrested. The vehicle was reported stolen out of San Francisco PD and was recovered and towed. Age of data: ~20 days.
 - a. Vehicle Data: 2005 Ford Econoline E350
12. 21-0111404; 03/13/2021 – Officers on patrol had an ALPR hit in the area of 45th Ave and E. 12th Street. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~1 day.
 - a. Vehicle Data: 2006 Nissan Maxima
13. 21-011572; 03/17/2021 – Officers on patrol had an ALPR hit on the 1300 block of E. 24th Street. The vehicle was unoccupied, attempts to contact the owner were successful, the vehicle was recovered and released to the owner. Age of data: ~4 days.
 - a. Vehicle Data: 2000 Honda CRV
14. 21-011654; 04/06/2021 – Officers on patrol had an ALPR hit on the 1600 block of Campbell Street. The vehicle was unoccupied, attempts to contact the owner were successful, but the vehicle was disabled, it was recovered and towed. Age of data: ~24 days.
 - a. Vehicle Data: 1994 Honda Civic
15. 21-011750; 03/30/2021 – Officers on patrol had an ALPR hit on the 1700 block of Marin Way. The vehicle was occupied, and a stop was conducted, with one individual being arrested for auto-theft. Attempts to contact the owner were unsuccessful, the vehicle was recovered and towed. Age of data: ~17 days.
 - a. Vehicle Data: 2001 GMC Yukon
16. 21-012745; 04/23/2021 – Officers on patrol had an ALPR hit on the 800 block of Chester Street. The vehicle was unoccupied, attempts to contact the owner were successful, and the vehicle was recovered and released to the owner. Age of data: ~1 month.
 - a. Vehicle Data: 1999 Honda Civic
17. 21-014081; 03/28/2021 – Officers on patrol had an ALPR hit on the 700 block of Wood Street. The vehicle was unoccupied and reported stolen by Hayward PD. The vehicle was recovered and towed. Age of data: ~5 days.
 - a. Vehicle Data: 1998 Ford Econoline

- 18.21-015106; 04/06/2021 – Officers on patrol had an ALPR hit on the 1600 block of 16th Street. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~3 days.
 - a. Vehicle Data: 1989 Toyota Pickup
- 19.21-026244; 06/10/2021 – Officers on patrol had an ALPR hit on the 1100 block of Chestnut Street. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~2 days.
 - a. Vehicle Data: 2003 Silver Nissan Altima
- 20.21-017449; 04/20/2021 – Officers on patrol had an ALPR hit on the 3200 block of Wood Street. The vehicle was unoccupied, attempts to contact the owner were successful, the vehicle was recovered and released to the owner. Age of data: ~3 days.
 - a. Vehicle Data: 2003 Chevy Silverado
- 21.21-018211; 04/25/2021 – Officers on patrol had an ALPR hit on the 3300 block of Helen Street. The vehicle was unoccupied, recovered, and towed. Age of data: ~4 days.
 - a. Vehicle Data: 1997 Honda Civic
- 22.21-018480; 04/23/2021 – Officers on patrol had an ALPR hit on the 1300 block of 5th Street. The vehicle was occupied, and a stop was initiated. An individual was detained and arrested. Attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~1 day.
 - a. Vehicle Data: 1993 Honda Civic
- 23.21-020648; 05/08/2021 – Officers on patrol had an ALPR hit on the 2700 block of 10th Avenue. The vehicle was unoccupied and inoperable, the vehicle was recovered and towed. Age of data: ~2 days.
 - a. Vehicle Data: 2000 Honda Accord
- 24.21-020912; 05/29/2021 – Officers on patrol had an ALPR hit on the 5500 block of Bancroft Avenue. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~22 days.
 - a. Vehicle Data: 1995 Honda Odyssey
- 25.21-035523; 07/31/2021 – Officers on patrol had an ALPR hit on the 2300 block of Embarcadero. The vehicle was moving and occupied, and a stop was conducted. Three suspects were detained with one being arrested for possession of a stolen vehicle. A stolen firearm was also recovered. The vehicle was recovered and released to the owner. Age of data: ~1 day.
 - a. Vehicle Data: 2007 White Mercedes CLK
- 26.21-025743; 06/12/2021 – Officers on patrol had an ALPR hit on the 550 block of 30th Street. The vehicle was unoccupied, recovered, and towed. Age of data: ~7 days.
 - a. Vehicle Data: 2003 Mazda Protégé
- 27.21-027162; 06/12/2021 – Officers on patrol had an ALPR hit while on the 550 block of 34th Street. The vehicle was confirmed to be reported stolen by Berkeley PD. The vehicle was unoccupied, attempts to contact the owner were successful, the vehicle, however, was inoperable and was recovered and towed. Age of data: ~5 days.
 - a. Vehicle Data: 1997 Honda Accord

- 28.21-027192; 06/12/2021 – Officers on patrol had an ALPR hit on the 550 block of 30th Street. The vehicle was confirmed to be reported stolen by Berkeley PD. The vehicle was unoccupied, recovered, and towed. Age of data: ~11 days
 - a. Vehicle Data: 1997 Honda Civic
- 29.21-031826; 07/12/2021 – Officers on patrol had an ALPR hit in the area of E. 15th Street and Miller Avenue. The vehicle was occupied and stopped with an individual being detained and arrested. Attempts to contact the owner were successful and the vehicle was recovered and released. Age of data: ~3 days.
 - a. Vehicle Data: 1992 Toyota Previa
- 30.21-033234; 07/28/2021 – Officers on patrol had an ALPR hit on the 200 block of 11th Avenue. The vehicle was unoccupied, attempts to contact the owner were successful, and the vehicle was recovered and released to the owner. Age of data: ~11 days
 - a. Vehicle Data: 2018 Volkswagen Tiguan
- 31.21-034757; 09/04/2021 – Officers on patrol had an ALPR hit in the area of 30th Street and Telegraph Avenue. The vehicle was unoccupied, attempts to contact the owner were successful, and the vehicle was recovered and released to the owner. Age of data: ~1 month
 - a. Vehicle Data: 1991 Honda Accord
- 32.21-036467; 08/23/2021 – Officers on patrol had an ALPR hit on the 1100 block of E. 15th Street. The vehicle (which was carjacked) was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~18 days.
 - a. Vehicle Data: 2015 Hyundai Veloster
- 33.21-037283; 08/10/2021 – Officers on patrol had an ALPR hit on the 1600 block of 62nd Avenue. The vehicle was reported as being carjacked by BART PD. The vehicle was unoccupied, recovered, and towed. Age of data: ~1 month
 - a. Vehicle Data: 2008 Toyota Corolla
- 34.21-039386; 08/23/2021 – Officers on patrol had an ALPR hit on the 2200 block of Embarcadero. The vehicle was occupied and stopped with an individual being detained and arrested. Attempts to contact the owner were successful and the vehicle was recovered, but the owner did not show up and the vehicle was towed. Age of data: Recovered same day.
 - a. Vehicle Data: 2002 Chevy Silverado 1500
- 35.21-040524; 08/29/2021 – Officers on patrol had an ALPR hit on the 3400 block of Elm Street. The vehicle was reported stolen out of Berkeley PD. The vehicle was unoccupied, inoperable, recovered, and towed. Age of data: ~5 days
 - a. Vehicle Data: 2002 Dodge RAM 2500
- 36.21-044190; 09/20/2021 – Officers on patrol had an ALPR hit in the area of 23rd Avenue and E. 11th Street. The vehicle was occupied and stopped with an individual being detained and arrested. The vehicle was reported stolen out of Emeryville PD. The vehicle was recovered and towed. Age of data: ~1 month
 - a. Vehicle Data: 2011 Ford F150

- 37.21-049102; 11/01/2021 – Officers on patrol had an ALPR hit on the 4000 block of Brookdale Avenue. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~12 days
 - a. Vehicle Data: 2007 Chevy Express Van
- 38.21-049863; 10/23/2021 – Officers on patrol had an ALPR hit on the 1200 block of 21st Avenue. The vehicle was reported stolen out of San Jose PD. The vehicle was occupied, and a stop was initiated, with two people being temporarily detained. An investigation discovered that the person who reported the vehicle stolen was not the registered owner and driver and passenger were released without further delay. Age of data: ~4 days
 - a. Vehicle Data: 2003 Toyota Corolla
- 39.21-051300; 11/01/2021 – Officers on patrol had an ALPR hit on the 4700 block of Bancroft Avenue. The vehicle was reported stolen by the Alameda County Sheriff's Office, was unoccupied, recovered and towed. Age of data: ~5 days.
 - a. Vehicle Data: 1993 GMC Sierra

Non-Stolen Vehicle Cases

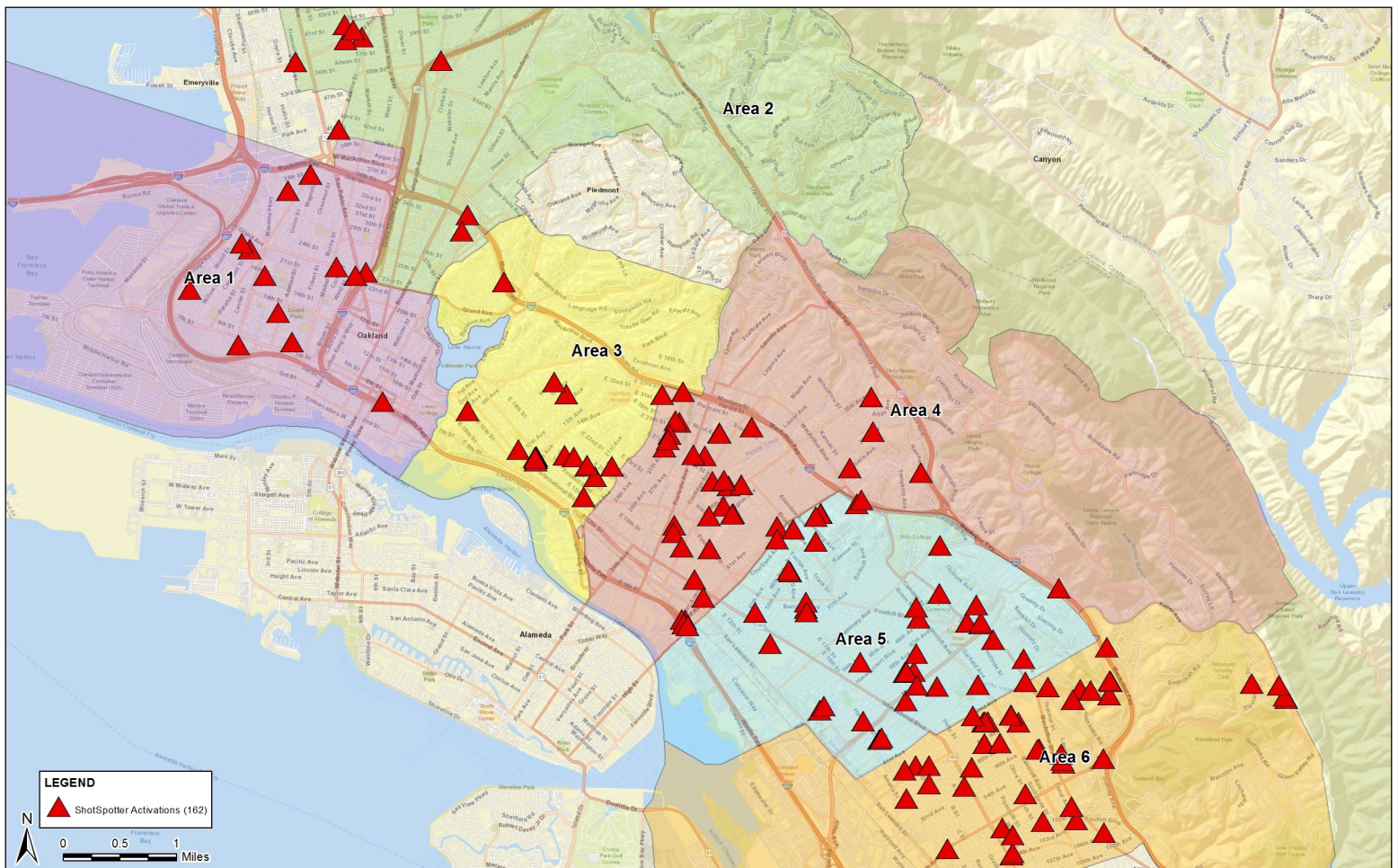
1. 21-012691; 03/19/2021 – ALPR was utilized to capture/scan license plates of vehicles participating in an illegal and unpermitted cabaret event party. Age of Data: Not Applicable
2. 21-012836; 03/20/2021 – ALPR was utilized by Pleasant Hill PD for a vehicle that was involved in an attempted murder. A stop was conducted, and an individual was detained and arrested. An illegal firearm was also recovered. Age of Data: ~6 days
3. 21-014039; 03/29/2021; – Officers on patrol had an ALPR hit on the 700 block of Walker Avenue. The vehicle was unoccupied, but the plate did not match the vehicle VIN it was attached to. The officer removed the plate and turned it into evidence. Age of data: 2 days.
4. 21-025695; 06/05/2021 – ALPR was utilized to search for a car that was suspected of being involved in a shooting. A warrant was obtained, and the individual was arrested. Age of data: ~1 month.
5. 21-031812; 07/09/2021 – Officers on patrol had an ALPR hit on the 7200 block of MacArthur Blvd for a vehicle involved in a robbery. The vehicle was occupied, a stop was attempted, and the suspects fled, eventually evading capture. Age of data: ~1 day.
6. 21-034075; 07/23/2021 – Officers on patrol had an ALPR hit on the 200 block of 29th Street. The vehicle was unoccupied, and the license plate was switched. The license plate was removed and attempts to contact the owner were unsuccessful. The license plate was remanded to evidence. Age of data: ~4 days.



Weekly ShotSpotter Activations Report — Citywide

14 Mar. – 21 Mar., 2022

ShotSpotter Activations	Weekly Total	YTD 2021	YTD 2022	YTD % Change 2021 vs. 2022
Citywide	162	2,091	2,003	-4%
Area 1	13	199	217	9%
Area 2	9	58	69	19%
Area 3	19	225	209	-7%
Area 4	36	327	352	8%
Area 5	40	722	575	-20%
Area 6	45	560	581	4%



All data sourced via ShotSpotter Insight.

Produced by the Oakland Police Dept. Crime Analysis Unit.



MEMORANDUM

TO: LeRonne Armstrong,
Chief of Police

FROM: Anwawn Jones, Sergeant
OPD, Intel Unit

SUBJECT: Cellular Site Simulator – 2021 Annual
Report

DATE: February 25, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology “Oversight following City Council approval” requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Oakland Police Department (OPD) Department General Order (DGO) I-11: Cellular Site Simulator (CSS) Usage and Privacy, requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and Public Safety Committee. The information provided below is compliant these annual report requirements.

Sergeant Anwawn Jones is currently the CSS Program Coordinator.

2021 Data Points

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

The Cell Site Simulator Surveillance (CSS) Impact report explains that, “Cellular site simulators, as governed by this policy, function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the simulator identify it as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would a networked tower.

CSS receives signals and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider to distinguish between incoming signals until the targeted device is located. Once the cellular site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone, rejecting all others.

The authorized purposes for using CSS interception technology and for collecting information using that technology to:

- a. *Locate missing persons*
- b. *Locate at-risk individuals*
- c. *Locate victims of mass casualty incidents*
- d. *Assist in investigations involving danger to the life or physical safety of an individual*
- e. *Apprehend fugitives*

The technology was requested one time in 2021. The request was part of the investigation into the fugitives involved in the shooting of a retired OPD Captain. The Alameda District Attorney's Office approved the use. However, officers discovered the suspects prior to use of the technology.

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

DGO I-11 does provide that OPD may share CSS data with other law enforcement agencies that have a right to know and a need to know¹, such as an inspector with the District Attorney's Office. However, no CSS data would be downloaded, retained, or shared. No data was generated or shared with any agency because it was not actually used in 2021.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

CSS is not attached to fixed objects.

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year.

CSS was not utilized anywhere in the City in 2021.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential

¹ DGO I-11 explains that a right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law.

greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

In terms of “an analysis shall also identify the race of each person that was subject to the technology’s use”:

- *The technology was not used, and therefore there was no data generated from usage;*
- *OPD does have information about the suspect(s) connected to the case that precipitated the technology request. However, the phone related to the considered usage could have been in possession of other people. The phone also could have been registered by a different person and/or registered using a pseudonym contact.*

For the reasons cited above, staff recommends that the PAC waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology’s impact on privacy interests is outweighed by the possible inaccuracy of the information potentially gathered in this situation.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information.

There were no uses in 2021 and thus no need for any audits. There were no policy violations.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

There were no uses in 2021 and thus no possible data breaches.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Table 1 below provides 2021 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2021 year.

Table 1: 2021 OPD Type 1 Crime Data

Part 1 Crimes <i>All totals include attempts except homicides</i>	01-01-2020 through 12-31-2020	01-01-2021 through 12-31-2021	Year-to-Date % Change 2020 vs. 2021	3-Year Year-to-Date Average	YTD 2021 vs. 3-Year YTD Average
Homicide - 187(a)	102	124	22%	100	24%
• Homicide - all other *	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• With Firearm	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• Auto	6,221	8,179	31%	8,921	-8%
• Residential	1,247	1,055	-15%	1,370	-23%
• Commercial	958	670	-30%	750	-11%
• Other/Unknown	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

- I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates.

There are no existing or new public records request for the 2021 calendar year.

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year.

Zero (\$0.00). OPD did not incur any maintenance, licensing, or training costs.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Reviewed by,
Roland Holmgren, Captain
OPD, Violent Crimes Operations Center

Prepared by:
Anwawn Jones, Sergeant
OPD, Intel Unit

Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Unit



MEMORANDUM

TO: LeRonne Armstrong,
Chief of Police

FROM: Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

SUBJECT: OPD Crime Lab Biometrics
DNA Analysis Technology
2021 Annual Report

DATE: March 11, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology “Oversight following City Council approval” requires that for approved surveillance technology items (by the Privacy Advisory Commission per OMC 9.64.020 and by City Council per OMC 9.64.030), city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the PAC, city staff shall submit the annual report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; or
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

The PAC recommended City Council adoption of the “Oakland Police Department (OPD) Criminalistics Laboratory DNA Instrumentation and Analysis Software Biometric Technology Use Policy on October 1, 2020; following the PAC’s vote, the City Council adopted Resolution No. 88388 C.M.S. on December 1, 2020. This resolution approved OPD’s use of Criminalistics Laboratory DNA Instrumentation and Analysis Software Biometric Technology. OMC 9.64.040 requires that, after City Council approval of surveillance technology, OPD provide an annual report for PAC review before submitting to City Council. This report is intended to serve to comply with this mandate.

2021 Data Details

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

General Overview

The Oakland Police Department (OPD) Criminalistics Laboratory’s (Crime Lab) Forensic Biology/DNA unit utilizes specialized DNA collection and analysis instrumentation and software to perform forensic DNA testing. During this lengthy and complicated process, one step removes and purifies DNA from cells (digestion/extraction), another quantitates how much DNA is present and lastly, by amplifying and analyzing Short Tandem Repeats (STR) in the DNA using Polymerase Chain Reaction (PCR) and separated by Capillary Electrophoresis (CE), forensic

DNA profiles are generated. Software is involved in the following processes: (i) collection and processing of STR DNA fragment data; (ii) interpretation of DNA data into DNA profiles used for comparison purposes. At the end of all processes, a determination can be made as to whether a DNA sample collected from a crime scene can be associated with a known individual through a comparison of evidentiary (crime scene) and known reference DNA profiles. Statistical weight is provided for all inclusion comparisons.

Specifics: How DNA testing was used in 2021

*The Forensic Biology Unit analyzed 430 (see **Attachment A for Case Record IDs**) requests between January 1, 2021 to December 31, 2021. Over 2,300 items of evidence were examined, from which 5,278 samples were subjected to digestion and extraction using the Versa and EZ1 instruments. Scientist subjected 5,425 samples to quantitation analysis using the SpeedVac, Qiagility, and QuantStudio 5 instruments and 2,196 samples were subjected to amplification and typing methods using the ProFlex and 3500 instruments. The DNA profiles were processed with GMIDX or FaSTR and ArmedXpert software.*

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

Discovery to the Alameda County District Attorney's Office was provided in 29 cases. A standard discovery packet includes the reports, technical and administrative review sheets, case notes, attachments, contact log, resume, interpretation guidelines, photographs, electronic data, and any supporting documents.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The Biometric Use Policy covers the specific technology covered. In general, the digestion, quantitation, normalization/amplification, typing, interpretation and databasing are housed in the laboratory of the Police Administration Building (PAB). Database equipment is located in a secure location elsewhere in the PAB as disclosed in the Use Policy. Currently, no equipment resides outside of these locations.

A cloud-based server location is under evaluation as a replacement for the server in the PAB. The details of this location and security would be handled under the auspices of the City of Oakland ITD policy and procedure and would meet or exceed industry standard for handling of secure servers.

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

All evidence was analyzed at the laboratory located in the PAB. No other locations are authorized. As for the geographic location of crimes, this is not collected by the laboratory in a way that can be disseminated easily. The address may be reported on the request for laboratory services form, but it is not required for analysis to proceed. The laboratory services crimes that occur in all areas of the City of Oakland.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review:

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

The laboratory request for services form does not collect race information. It could be argued that requiring information that is not necessary for analysis, such as race, could be biasing; indeed, it would be a great invasion of privacy to capture this data since it is irrelevant to the analyses performed. Furthermore, the race of individuals subject to the DNA analysis technology's use is not revealed during evaluation of evidence as non-coding regions of DNA are typed and do not contain this information. Therefore, staff recommends that the PAC waive the requirement to identify the race of each person subject to the technology's use and make a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the potential greater invasiveness in capturing such data.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy (SUP), and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

All Forensic Biology personnel and relevant management were required to review and sign that they understood and would abide by the Surveillance Use Policy and the Impact Reports. Under accreditation, the Laboratory actively seeks feedback from its customers and no concerns were conveyed regarding violations or concerns around the SUP. Lastly, the Laboratory has a means to identify risks through Incident Response. Staff are encouraged to participate in Incident Response by filing Incident Alerts where there were concerns. No violations or potential violations were identified by any of these routes.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

The laboratory maintains an active security program where the security of alarmed portions of the laboratory are tested and results recorded. There were no unexplained alarm events and there were no faults in the alarmed systems that were tested. There were no breaches to the laboratory nor to the equipment or databases that it houses. More importantly, there were no electronic data breaches in the laboratory.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

The efficacy of the OPD Criminalistics Laboratory DNA analysis program is illustrated by citing the following compelling statistics:

The laboratory completed 430 requests in 2021. These are further broken out by crime type in Table 1 below

Table 1: OPD Crime Laboratory DNA Analysis Requests in 2021

Crime Type	Number of Requests
Homicide	92
Attempted Homicide	18
Cold Case Homicide	2
Suspicious Death	1
Rape	114
Other Sexual Assault (not rape)	57
Kidnapping	1
Assault	49
Robbery	29
Burglary	12
Carjacking	9
<i>Hit and run</i>	2
Auto Theft	1
Weapons	35
Other Person	4
Other Criminal	3
Officer Involved Shooting	1
Total	430

CODIS hits in 2021 – One hundred and twenty-four DNA profiles were uploaded to the CODIS database. The laboratory had one hundred and seventeen associations (hits); seventy-two hits to named individuals whose identity were unknown, seven hits to unsolved forensic cases, and thirty-eight hits to previously solved forensic cases.

Thus, forensic DNA analysis is an important tool to investigate and provide potential leads for a variety of crimes that occur in the City of Oakland.

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There were no public record requests for DNA analysis.

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Procurement of instruments is costly and is typically amortized over many budget cycles. Ongoing maintenance is imperative to ensure reliability of the instruments is remediated quickly should a problem occur. The reagents/kits and supplies to conduct testing are also steep. The cost / benefit analysis in the form of Return on Investment (ROI) calculations place the societal cost of each homicide at \$10,000,000 and a return seen of \$135¹ per dollar spent on violence reduction. Similarly, economic studies show that investigating sexual assaults results in \$81² saved per dollar spent.

The total costs of procuring and maintaining the equipment are shown by Category of testing and platform below:

Digestion/Extraction

- EZ1: \$63,000 to purchase (x3 instruments = \$189,000) and \$3,100 to maintain; 3 instruments for \$9,300 annual*
- Versa 1100: \$85,000 to purchase and \$6,800 to maintain*

DNA Quantitation

- Qiagility: \$33,100 to purchase (x3 instruments = \$99,300) and \$2,700 to maintain; 3 instruments for \$8,100*
- QuantStudio 5: \$57,000 to purchase (x2 instruments = \$114,000) and \$5,100 to maintain; 2 instruments for \$10,200*

DNA Normalization / Amplification

SpeedVac: \$4,000 to purchase, no maintenance

ProFlex Thermalcyclers: \$14,000 to purchase (x2 instruments = \$28,000), no maintenance

DNA Typing

3500: \$135,000 to purchase, \$6,000 to maintain

DNA Interpretation

STRmix: \$66,000 to upgrade, \$22,000 to maintain

FaSTR: \$37,000 to purchase, \$8,000 to maintain

ArmedExpert: \$15,000 to purchase

¹ Abt, Thomas (2019). Bleeding Out: The devastating consequences of urban violence—and a bold new plan for peace in the streets. Chapter 11, p. 208.

² Wang and Wein (2018) Journal of Forensic Sciences, Analyzing Approaches to the Backlog of Untested Sexual Assault Kits in the USA, July 2018, Vol. 63, No. 4, pp. 1110-1121.

The cost of testing reagents/kits was approximately \$131,000, however, this does not include consumables such as scalpels, masks, gloves, plastics, slides nor serological test kits.

*Total purchase cost (born over several years): \$772,300
Total maintenance cost, 2021: \$70,400
Total testing cost reagents/kits, 2021: \$131,000
Estimate of consumables: \$140,000*

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

The instruments and software listed in the September 2020 Surveillance Impact Report (SIR) and Biometric Technology Use Policy (SUP) were not replaced during 2021. The laboratory did take some instruments and software out of service and replaced with technology platforms already included in the SIR and SUP (e.g. the Proflex and 3500 instruments).

For the current year, the laboratory is in the process of replacing the three Qiagen EZ1 robots (14 sample capacity) with two EZ2 robots. The EZ2 robot has a larger capacity (24 sample capacity) and will increase the number of samples processed in the same amount of time. The EZ2 robots were purchased with FY2020 Capacity Enhancement and Backlog Reduction (CEBR) grant funds as declared in resolution 88358 for which purchase permission was granted; they are ordered, and the laboratory awaits shipment.

Later this year, when FY2021 CEBR grant funds become available, four cold storage units (freezer/refrigerator and refrigerator) will be replaced as declared in resolution 89011. The laboratory is also in the planning stages for STRmix software validation which has been disclosed in the existing SIR and SUP.

No new biometric capacities were added to the laboratory during 2021. The laboratory is proposing a few changes to the current SUP and SIR 1) to reflect the technology that has been retired or replaced and 2) to add language codifying current OPD criminalistics laboratory practices which prevent improper use of victim profiles.

Edits in the SUP and SIR address retired or replaced technology.

Codification of Prevention of Improper use of Victim Profiles

In the past, the Forensic Biology unit QC database contained DNA profiles obtained from blood samples associated with homicides, suspicious circumstance deaths, and sexual assault cases. These blood samples were anonymized, assigned a QC source number and used as positive control samples for casework analysis. The purpose of using these QC samples was to show that the testing method or DNA typing process worked by verifying that expected results were obtained. This process was performed from 1996 to 2011. In 2012, the anonymized DNA profiles obtained from these samples was included in the QC database described above for the purpose of quality checks of backlogged or re-sampled

cases. The source of the profiles is unknown to crime lab line staff. They have never been, nor will they ever be, used for the identification of an individual in a criminal matter. Nevertheless, and in an abundance of caution, these QC samples were removed from the active database and archived in a location only accessible by FBU Supervisors. Additionally, language specifying that these profiles cannot be used for associations is proposed to be added to the SUP.

The Forensic Biology unit maintains an in-house Quality Control (QC) database. The QC database contains DNA profiles obtained from the following sources:

- 1. By consent from OPD staff (current and past) and their family members. OPD personnel that may enter the chain of custody for an evidence item or has other contact within the scope of the case,*
- 2. Samples provided by accredited proficiency test providers. The samples are anonymized by the test provider; the test providers are subject to strict confidentiality requirements by the accrediting bodies. The laboratory has no access to the source of these samples.*
- 3. The purpose and use of the QC database is twofold: 1) for casework quality control checks to ensure that the process worked correctly (positive control) and 2) to determine if there is possible contamination from a known individual to a casework sample. At this time, there are no victim references in the QC database. Such profiles have never been, nor are they allowed to be, used for the identification of an individual in a criminal matter.*

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

For any questions with this report, please contact Dr. Sandra Sachs, Criminalistics Laboratory Manager, at ssachs@oaklandca.gov.

Respectfully submitted,

Reviewed by,
Drennon Lindsey,
Deputy Chief, Bureau of Investigations

Prepared by:
Sandra Sachs, PhD, Crime Lab Manager
OPD, Criminalistics Laboratory

Bonnie Cheng, Acting Forensic Biology Unit Supervisor
OPD, Criminalistics Laboratory

Bruce Stoffmacher, Privacy and Legislation Manager
OPD, Bureau of Services

Attachments (1)

A: Criminalistics Laboratory - Requests Completed Between 01 Jan 21 and 31 Dec 21



MEMORANDUM

TO: LeRonne L. Armstrong,
Chief of Police

FROM: Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

SUBJECT: Forensic Logic CopLink
System – 2021 Annual
Report

DATE: March 22, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology “Oversight following City Council approval” requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Oakland Police Department (OPD) Department General Order (DGO) I-24: Forensic Logic CopLink, as well as OMC 9.64.040 together require that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and Public Safety Committee. The information provided below is compliant with these annual report requirements.

DGO I-24 explains that authorized members may use CopLink for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

Captain Paul Figueroa, Criminal Investigations Division Commander, was the Program Coordinator for 2021.

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

Forensic Logic search technology is used regularly by both OPD sworn field / patrol personnel and command staff. Search parameters include the following criteria which are submitted to a search engine where data originating from law enforcement records, calls for service, field interviews, arrest/booking records and citations are stored:

- *License plate numbers*

- *Persons of interest*
- *Locations*
- *Vehicle descriptions*
- *Incident numbers*
- *Offense descriptions/penal codes*
- *Geographic regions (e.g., Police Beats or Police Areas)*

Data is stored in an FBI Criminal Justice Information Service (CJIS) compliant repository in the Microsoft Azure GovCloud and encryption of data both at rest and in transit is protected by being compliant with FIPS 140-2.

In 2021, there were a total of 573 distinct users who conducted Forensic Logic searches, for a total of 498,267 separate queries. Table 1 below breaks down this search data by month and by distinct user and total searches.

Table 1: OPD CopLink Searches; by Distinct User and Search Totals

Search Type	January	February	March	April	May	June
<i>Number of OPD distinct users in each month</i>	345	352	345	359	365	366
<i>Number of searches conducted</i>	41,665	46,601	45,940	47,718	43,929	40,302

Search Type	July	August	September	October	November	December
<i>Number of OPD distinct users in each month</i>	342	336	342	334	313	307
<i>Number of searches conducted</i>	40,141	42,506	36,149	45,949	33,725	33,642

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

Data searched with the Forensic Logic CopLink system is entirely acquired from incident reports, citations, calls for service and field interviews that have already been recorded in originating Records Management Systems, Computer Aided Dispatch Systems, and Mobile Field Reporting Systems – from both OPD systems as well as from other law enforcement agency systems (other Forensic Logic client agencies). The data is collected from OPD systems at least once every 24 hours; once the data is collected and resides in the Forensic Logic cloud repository, it is made available to agencies subscribing to the Forensic Logic service who are permitted by their agency command staff to access CJIS information¹.

¹ Below is the warning message on the service user sign-on page that every user sees prior to accessing the system:

Data sourced from the Oakland Police Department cannot be accessed by US DHS ICE nor US DHS CBP staff.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to.

The CopLink service is accessible by authorized OPD users on OPD computers with appropriate an user-id and password (criteria for both defined by FBI CJIS Security Addendum). OPD data sources that provide data accessible to the search tool include the following:

- *Arrest records*
- *Field contacts*
- *Incident reports*
- *Service calls*
- *Shots fired (ShotSpotter)*
- *Stop Data reports*
- *Traffic Accident reports*

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

CopLink software is not deployed in a manner as is physical hardware technology. The software is used by OPD personnel at the Police Administration Building, Eastmont Building, Communications Center, the Emergency Operations Center, (when active) and in patrol vehicles to search crime incidents and related data. The data itself can relate to crime data with geographic connections to anywhere in the City as well as the broader region and even nationally.

WARNING: You are accessing sensitive information including criminal records and related data governed by the FBI's Criminal Justice Information System (CJIS) Security Policy. Use of this network provides us with your consent to monitor, record, and audit all network activity. Any misuse of this network and its data is subject to administrative and/or criminal charges. CJIS Security Policy does not allow the sharing of access or passwords to the Forensic Logic Coplink Network™. The data content of the Forensic Logic Coplink Network™ will not be considered for use as definitive probable cause for purposes of arrests, searches, seizures or any activity that would directly result in providing sworn testimony in any court by any participating agency. Information available in the Forensic Logic Coplink Network™ is not probable cause, but indicates that data, a report or other information exists in the Records Management System or other law enforcement, judicial or other information system of an identified participating agency or business.

In accordance with California Senate Bill 54, applicable federal, state or local law enforcement agencies shall not use any non-criminal history information contained within this database for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. §§ 1373 and 1644.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

OPD is not able to provide the race of each person connected to each CopLink query. There are thousands of queries and not all queries would provide race data of each suspect or person connected to each data result. Staff therefore recommend that the PAC makes the determination, that the administrative burden in collecting or verifying this information as well as the associated potential for greater invasiveness in capturing such data outweighs the public benefit.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

Forensic Logic conducted an audit of OPD system queries to ensure all logins were conducted by existing OPD personnel

Forensic Logic is notified of additions or deletions to its subscription services by the designated Point of Contact at the Oakland Police Department. Forensic Logic also would modify the user census upon the request of any Chief of Police, Assistant Chief of Police or Deputy Chief of Police of the Oakland Police Department.

In addition, all Oakland Police Department users can only use Forensic Logic services from within OPD designated facilities such as the Police Administration Building, the Eastmont satellite location, the Communications Center, the Emergency Operations Center and from inside a patrol vehicle due to Forensic Logic's requirement that Internet Protocol (IP) addresses for users be whitelisted (be enabled for access). Any attempt to log in to the Forensic Logic services outside of those locations would fail by any person with an authorized OPD user id (email address).

In addition, on an annual basis, Forensic Logic will prepare a list of enabled OPD users for review by the OPD Point of Contact to confirm that all users should be enabled for access to the Forensic Logic services. Should individuals need to be removed from the services, the Point of Contact will notify Forensic Logic at that time.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

Neither OPD, Oakland Information Technology Department, nor Forensic Logic are aware of any data breaches.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

Table 1 below provides 2021 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2021 year

Table 1: 2021 OPD Type 1 Crime Data

Part 1 Crimes <i>All totals include attempts except homicides</i>	01-01-2020 through 12-31-2020	01-01-2021 through 12-31-2021	Year-to-Date % Change 2020 vs. 2021	3-Year Year-to-Date Average	YTD 2021 vs. 3-Year YTD Average
Homicide - 187(a)	102	124	22%	100	24%
• Homicide - all other *	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• With Firearm	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• Auto	6,221	8,179	31%	8,921	-8%
• Residential	1,247	1,055	-15%	1,370	-23%
• Commercial	958	670	-30%	750	-11%
• Other/Unknown	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

- I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There are no existing or newly opened public records requests relating to Forensic Logic, CopLink, or LEAP (former name for CopLink).

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Tables 2 and 3 below provides costing data from the current Oakland Forensic Logic contract.

Table 2: Oakland Forensic Logic Contract Cost; July 2020 - June, 2022

For the Period 07/01/2020 through 06/30/2022 payable upon execution of agreement:

Product Number	Description	List Price	Sales Price	Quantity	Subtotal	Discount (%)	Total Price
	CopLink SEARCH (07/01/20-06/30/21)	\$275	\$199	794	\$158,006	0%	\$158,006
	CopLink Analytics (07/01/20-06/30/21)	\$1,000	\$1,000	794	\$794,000	100%	\$0
	CopLink CONNECT (2 Years)	\$20,000	\$20,000	1	\$20,000	0%	\$20,000
	Integration Services NIBIN	\$5,000	\$5,000	1	\$5,000	0%	\$5,000
	Integration Services Motorola Premiere One CAD and RMS	\$25,000	\$25,000	1	\$25,000	0%	\$25,000
	CopLinkX (07/01/21-06/30/22)	\$275	\$275	794	\$218,350	0%	\$218,350
	Integration and Maintenance Services	\$25,000	\$25,000	1	\$25,000	0%	\$25,000
	Round down discount		(\$356)	1	(\$356)		(\$356)
						TOTAL	\$451,000

Table 3: Oakland Forensic Logic Contract Cost; July 2022 - June, 2023

For the Period 07/01/2022 through 06/30/2023 payable on July 1 2021:

Product Number	Description	List Price	Sales Price	Quantity	Subtotal	Discount (%)	Total Price
	CopLink SEARCH						
	CopLink Analytics						
	CopLink CONNECT	\$10,000	\$10,000	1	\$10,000	0%	\$10,000
	CopLinkX	\$275	\$275	794	\$218,350	0%	\$218,350
	Integration and Maintenance Services	\$25,000	\$25,000	1	\$25,000	0%	\$25,000
	Round down discount		(\$350)	1	(\$350)		(\$350)
						TOTAL	\$253,000

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

Drennon Lindsey, Deputy Chief of Police
OPD, Bureau of Investigations

Reviewed by,
David Elzey, Captain
OPD, Criminal Investigations Division

Prepared by:
Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Unit



MEMORANDUM

TO: LeRonne Armstrong,
Chief of Police

FROM: Robert Rosin
Acting Captain of Police

SUBJECT: Pursuit Mitigation System – 2021
Annual Report

DATE: February 22, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology “Oversight following City Council approval” requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Oakland Police Department (OPD) Department General Order (DGO) I-22: Pursuit Mitigation System requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and Public Safety Committee. The information provided below is compliant with the annual report policy requirements of DGO I-22 as well as OMC 9.64.040.

Acting Captain Rosin, Bureau of Field Operations I, Area 2, is currently the Pursuit Mitigation System Coordinator.

DGO I-22 explains that “StarChase,” a private company, manufactures and supports its Pursuit Mitigation GPS Tag Tracking System. The “StarChase” system is a pursuit management technology that contains a miniature GPS tag and a launcher mounted in a police vehicle. The GPS Tag and Track Launcher System are comprised of a less-than-lethal, dual barrel GPS launcher which contains two GPS Tags (1 per barrel) mounted in the vehicle grille or on a push bumper. The launcher is equipped with compressed air and an eye-safe laser for assisting with targeting before launching the GPS Tag.

2021 Annual Report Details

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

GPS Tag technology was deployed one (1) time in 2021. On New Year’s Eve 2021, OPD received information of an armed caravan assembling in a West Oakland neighborhood. Plain clothes officers were dispatched to the area to investigate and make observations from a safe distance. A suspect vehicle from a previous armed caravan incident was observed. The vehicle left the area and separated from the

caravan. OPD personnel attempted a traffic stop, but the suspect vehicle evaded OPD patrol vehicles; no pursuit was initiated or authorized. Later, an OPD officer was able to position the patrol vehicle behind the suspect vehicle. OPD Command approved the deployment of the GPS Tag in order to assist in the safe apprehension of the suspect. One GPS Tag was launched at the rear of the vehicle but failed to affix properly and subsequently fell off the vehicle. There was no active tracking yielded from the GPS Tag deployment.

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

No GPS Tag data was generated from this one use.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

n/a

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

The technology was deployed on Interstate 80 near the city of Vallejo, outside of the City of Oakland.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff. The suspect connected to the vehicle where the GPS Tag Tracker was deployed was (one) male African American.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

There were no audits as the technology was deployed only once, the use was in alignment with DGO I-22, and no data was generated.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

There were no Pursuit Mitigation System technology data breaches as there was no data generated.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

Table 1 below provides 2021 Part 1 Crime Data. The Crime Data report shows the high level of many types of Type 1 violent crimes occurring throughout the City. OPD uses surveillance technology to address this high level of crime.

Part 1 Crimes <i>All totals include attempts except homicides</i>	01-01-2020 through 12-31-2020	01-01-2021 through 12-31-2021	Year-to-Date % Change 2020 vs. 2021	3-Year Year-to-Date Average	YTD 2021 vs. 3-Year YTD Average
Homicide - 187(a)	102	124	22%	100	24%
• Homicide - all other *	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• With Firearm	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• Auto	6,221	8,179	31%	8,921	-8%
• Residential	1,247	1,055	-15%	1,370	-23%
• Commercial	958	670	-30%	750	-11%
• Other/Unknown	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

- I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There were no public records requests (open or closed) related to GPS Tag technology in 2021.

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

OPD anticipates that the annual cost – once deployed – will be approximately \$30,000 annually for unlimited data and mapping service. This expense will be supported from OPD's database subscription account.

- K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for changes at this time.

While there was just one deployment of the GPS Tag system in 2021, OPD Command Staff has a plan to re-highlight the importance of the use of the GPS Tag technology as it relates to pursuit mitigation. The Training Section will produce a video which demonstrates the use of the GPS tag system and covers some of the relevant policy points which will help officers remember to request/use the technology during stressful enforcement action when split-second decisions are crucial. Additionally, OPD will move all vehicles equipped with the GPS Tag systems to the Patrol Division. Patrol Officers are engaged with more pursuits than other units because they have fewer resources available to follow and are more often responding to crimes in progress than special duty teams.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments as well as the reporting requirements of OMC 9.64.040. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

Robert Rosin, Acting Captain
OPD, Bureau of Field Operations 1, Area 2

Reviewed by,
Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Roland Holmgren, Captain
OPD, Violent Crime Operations Center

Prepared by:
Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Section



MEMORANDUM

TO: LeRonne Armstrong,
Chief of Police

FROM: Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

SUBJECT: Mobile Fingerprint ID– 2021
Annual Report

DATE: March 15, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology “Oversight following City Council approval” requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

The City Council adopted Resolution 88095 C.M.S. on April 7, 2020 which approved the OPD Mobile ID Surveillance Use Policy as well as the Surveillance Impact Report.

OPD does not currently possess any Mobile Identification Devices (MID)s and there was zero (0) MID usage by OPD in 2021. The Alameda County Sheriff’s Office (ACSO), the lead sponsor of the MID program, is currently upgrading the devices with technology provider. OPD will appoint an internal MID Coordinator when OPD is able to receive and deploy upgraded units.

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

The Surveillance Impact Report for the Mobile Identification Device MID explains that, “Mobile Identification Devices (MID) are small enough to be handheld, and contains an optical sensor to scan fingerprints and transmit them to look for matches within local databases MIDs are not investigative tools – they only allow personnel to attempt to match fingerprints of individuals who are to be arrested with possible matches from past arrests in Alameda and Contra Costa Counties.

The MID uses the Bluetooth radio standard to send a scanned image of a fingerprint to a police vehicle mobile data terminal (MDT), which can connect with special software. The software accesses a regional fingerprint database shared by Alameda and Contra Costa Sheriff’s Offices called Cogent Automated Fingerprint Identification System (CAFIS).

The sole purpose of the MID is to allow police to identify individuals who do not possess acceptable forms of identification (e.g. driver's license or passport) in cases where they otherwise do not need to be booked in the Alameda County Jail. State law requires police to identify individuals to be cited for an infraction or misdemeanor; arrest and booking into jail is legally required when an acceptable form of ID cannot be obtained. Police need to know who you are when a citation is appropriate."

OPD did not possess nor deploy MIDs in 2021.

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

There was no usage and no data generated in 2021.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

MIDs are not attached to any fixed objects.

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

OPD did not deploy MIDs anywhere in the City in 2021.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

There was no usage of MIDs and no data or usage to audit.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

There was no MID-related data generated and no data breaches.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

Non applicable based on zero usage.

- I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

No public records requests related to MIDs in 2021.

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

There was no MID usage and no cost to OPD.

- K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Reviewed by,
Jeffrey Thomason, Lieutenant
OPD, Special Operations Section

Prepared by:
David Pullen, Officer
OPD, Bureau of Services, Information Technology Unit

Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Unit



MEMORANDUM

TO: LeRonne Armstrong,
Chief of Police

FROM: Trevelyon Jones, Captain,
Ceasefire Section

SUBJECT: Gunshot Location Detection
System (ShotSpotter) – 2021
Annual Report

DATE: March 22, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology “Oversight following City Council approval” requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

The PAC recommended adoption of OPD Department General Order (DGO) I-20: “Gunshot Location Detection System” at their October 3, 2019 meeting; the report was presented to the City Council on November 19, 2019 and adopted by the City Council via Resolution No. 87937 C.M.S. DGO I-20 requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council.

2021 Data Details

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

From the “Surveillance Impact Use Report for the Gunshot Location Detection System:”

Part 1 – How the System Works: “The GLD system sensors are designed to detect gunshots based on their acoustic signature (e.g. broad-frequency, impulsiveness and loudness). The utilization of multiple sensors at different distances from a gunshot sound allows the system not only to capture the sound but assign a probability that it is a gunshot and triangulate its precise location based on time difference of arrival. If the machine classifier in the “ShotSpotter Cloud” determines it is likely a gunshot based on computer-learning algorithms, the system will pull a short audio snippet from the sensors that detected it and send it to human analysts at the ShotSpotter Incident Review Center at its headquarters in Newark, CA. The analysts perform an auditory and visual assessment of the audio waveform to make a final determination as part of a two-phased classification process. If confirmed as a gunshot, an alert is published containing

information such as street address, number of rounds fired, and a short audio snippet of the gunfire event– all within 60 seconds of the trigger pull (29 seconds on average).”

From Section 2: Proposed Purpose: “The purpose of GLD is to enable OPD to provide a higher level of the service to the community related to shootings. The system detects, locates and alerts officers of virtually all gunshots in a coverage area in less than 60 seconds enabling officers to respond to and investigate gunshots incidents they would not have known about and to respond to them much more rapidly than waiting for a 911 call. Personnel can better respond to gunshot activity and respond to possible armed individuals as well as to possible gunshot victims through this important real-time data.”

ShotSpotter technology was used in the following ways/with the following outcomes in 2021:

- *The number of times ShotSpotter technology was requested: ShotSpotter alerted OPD to 8,965 unique gunshot incidents from January 1 – December 31, 2021. Of those alerts, 8,922 (99%) were not called in by the community as a 415GS call type (shots fired), and OPD would not have known about them nor have been able to respond in a timely fashion. This information is based on an analysis of calls within 15 minutes and 300 feet of a ShotSpotter alert.*
- *ShotSpotter led police to 86 shooting victims when no one called 911, 10 of which were homicides and 76 were injured. OPD was able to provide and coordinate immediate emergency medical response to the 76 surviving shooting victims; OPD personnel believe that several of these victims survived the shootings specifically because of the quick response subsequent medical attention. In some instances, OPD and medical response occurred within less than two minutes of the ShotSpotter activation. The ShotSpotter alert was within 10 minutes and 1,000 feet of the location where the victim was found. Furthermore, staff believe that there were many more cases where OPD responded to activations and found shooting victims – and where critical medical attention was provided. The 86 cases cited here (76 injury cases) are the ones where OPD and ShotSpotter staff can conclusively cite the response to the ShotSpotter activations.*
- *ShotSpotter activations led OPD to 67 victims where their vehicle and/or dwelling was shot. Of these 67 victims, 28 victims were present but not hit by gunfire, and 39 were listed as victims because the property belonged to them.*
- *1,530 crime incident reports (17% of total activations)*
 - *1,108 (72%) of these incidents resulted in OPD Crime Lab requests for further firearm forensic analysis.*
- *ShotSpotter provided the following additional reports in relation to specific ShotSpotter activations:*
 - *Seventeen detailed forensic reports*
 - *Court preparation for eight cases*

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

The following agencies have been provided log-in access to the ShotSpotter System for ongoing usage:

1. *OPD and the Oakland Housing Authority Police Department entered into a Memorandum of Understanding (MOU) in 2012, following City Council approval, to fund the initial ShotSpotter program in areas of the City and near OHA buildings known for higher levels of gun shots. This MOU allows OPD to share access to the ShotSpotter cloud-based portal with OHA PD personnel.*
2. *Personnel from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) who participate in the Council-approved OPD-ATF Taskforce also have access to the ShotSpotter System.*

These agencies have ongoing log-in access and do not make written requests for access.

DGO I-20 Section B – 1. “Authorized Use” states:

The Chief of Police or designee shall provide necessary training and/or technical assistance for GLD usage. Only OPD personnel, authorized members of agencies working in contracted partnership with OPD, and members of agencies specifically designated for temporary authorization by the Chief of Police, shall be granted access to OPD’s GLD System. The Chief of Police may designate temporary authorization to utilize OPD’s GLD system to members of agencies working in partnership with OPD within the City of Oakland.

The California Highway Patrol (CHP) requested ShotSpotter access during the May Day event in 2021 when there were hundreds of people at large events in the downtown area. However, command approval was not granted in time for this request; ultimately, no access was granted.

Separate from ongoing login access, DGO I-20 provides rules for sharing ShotSpotter System data with outside agencies. Section C–3 of DGO I-20: “GUNSHOT LOCATION DETECTION SYSTEM” – “Releasing or Sharing GLD System Data,” states:

“GLD system data may be shared only with other law enforcement or prosecutorial agencies based on a need to know or a right to know, or as otherwise required by law, using the following procedures:

1. *The agency makes a written request for the ShotSpotter data that includes:*
 - a. *The name of the requesting agency.*
 - b. *The name of the individual making the request.*
 - c. *The need for obtaining the information.*
2. *The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.*
3. *The approved request is retained on file and shall be included in the annual report.*

OPD did not provide specific ShotSpotter data to outside law enforcement agencies in 2021. However, OPD investigators in the Criminal Investigations Division and or other sections of OPD such as the Ceasefire Section regularly communicate with personnel from other law enforcement agencies on interjurisdictional investigations; these forms of collaboration may involve discussions related to shootings where OPD became informed from ShotSpotter

activations. ShotSpotter activations many times may lead to evidence gathering (e.g., finding bullet casings); OPD may share information about evidence (e.g., that bullet casings were found in a particular area at a particular time).

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

OPD has contracted with ShotSpotter to install GLD sensors in different areas (phases) in several parts of the city. The total coverage area for the current ShotSpotter system comprises 18.17 square miles or approximately 32 percent of the city land size (55.93). OPD has chosen to install the sensors in areas most prone to gunshots based upon historical data. Many areas in East and West Oakland now benefit from the GLD system.

Most sensors are placed approximately 30 feet above ground level to maximize sound triangulation to fixed structures (e.g., buildings); at this altitude, the sensors can only record limited street-level human voice sounds. Furthermore, ShotSpotter only retains the audio for one second prior to a gun shot, and one second after.

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

Attachment A to this report provides the geographic areas of the City of Oakland that comprise the three ShotSpotter “phases” or areas covered under the current OPD-ShotSpotter contract. These areas intersect with all five official OPD Police Areas with a focus on areas where gunfire has historically occurred with greater regularity. **Attachment B** to this report is a weekly public ShotSpotter Activation Report for the week of March 22-28, 2021; this later report highlights areas of Oakland where ShotSpotter alerts have most recently occurred.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology’s adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology’s use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology’s impact on privacy interests is outweighed by the City’s administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

OPD is not able to provide the race of each person connected to each activation since shooting suspects are often unknown. Many times, there is data regarding the race of shooting victims or witnesses (may be self-reported); however, this data is not captured in the same system as ShotSpotter and the administrative burden (6,053 total 2021 activations) to constantly connect the two disparate datasets would overwhelm staff capacity. OPD therefore recommends that the PAC makes the determination, that the administrative burden in collecting or verifying this information as well as the associated potential greater invasiveness in capturing such data outweighs the benefit.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

New officers and crime analysts are trained on the ShotSpotter System as part of police officer academies. Officers and analysts are provided direction that covers login, and how to use different views (e.g., time-period).

OPD officers have automatic access to ShotSpotter notifications when in patrol vehicles equipped with standard vehicle computers via the ShotSpotter Respond System. ShotSpotter creates a log for every sign-in to their system, which includes the level of access the user has (admin view or dispatch view, which is notification only). OPD and ShotSpotter has verified that for 2021, all users who logged into the system were authorized users.

Patrol Officers in vehicles and/or on mobile phones utilize the ShotSpotter Respond System. The Respond System pushes notifications to users – there is no interactivity functionality. Shotspotter can only audit logins for both the Respond and the Insight program. ShotSpotter and OPD staff have verified that all logins were associated with appropriate active employees. Staff regularly removes access from employee emails where staff separate from City employment.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

Neither OPD, ShotSpotter, nor the city's IT Department are aware of any data breaches of ShotSpotter data or technology in 2021.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Table 1 below provides 2021 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2021 year

Table 1: 2021 OPD Type 1 Crime Data

Part 1 Crimes <i>All totals include attempts except homicides</i>	01-01-2020 through 12-31-2020	01-01-2021 through 12-31-2021	Year-to-Date % Change 2020 vs. 2021	3-Year Year-to-Date Average	YTD 2021 vs. 3-Year YTD Average
Homicide - 187(a)	102	124	22%	100	24%
• Homicide - all other *	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• With Firearm	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• Auto	6,221	8,179	31%	8,921	-8%
• Residential	1,247	1,055	-15%	1,370	-23%
• Commercial	958	670	-30%	750	-11%
• Other/Unknown	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

Table 2: ShotSpotter Activations Resulting in Incident Report for Firearm Crimes by Category in 2021

Cases by Firearm-Related Crime Type	No.
Homicide	27
Attempted Homicides	6
Assault with a Firearm	186
Shoot at an Occupied Home/Vehicle	93
Shoot at an Unoccupied Home/Vehicle	88
Negligent Discharge of a Firearm	1,076
Weapons Violations (including exhibit/draw)	11
Robbery with a Firearm	10
Other (non-firearm crime type)	29
Total Cases	1,530

Table 3: Firearm Recoveries in 2021 Connected to ShotSpotter Activations illustrate Guns Recovered

Firearm-Related Crime Type	No.
Homicide	15
Assault with a Firearm	31
Shoot at an Occupied Home/Vehicle	3
Shoot at an Unoccupied Home/Vehicle	1
Negligent Discharge of a Firearm	17
Weapons Violations (including exhibit/draw)	18
Battery	0
Oher (non-firearm related)	3
Total Cases	88

- 88 weapons seized.
 - Note: more than one firearm may be from the same incident.
- 700 incidents when advanced situational awareness was provided to responding patrol officers on their way to crime scenes in high danger situations that required specific approach tactics such as multiple shooters, high capacity or automatic weapons being used, and drive-by shootings.

Table 4: Cases Where ShotSpotter Notifications Resulted in Gunshot Victim Medical Support

Dispositions	Incidents
Murder	10
Assault Firearm	75
Attempted Murder	1
Total Cases	86

- I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There are six existing and/or new (five current) public records requests (PRR) in 2021.

1. RT – 16562
2. RT – 20137
3. 18-4226
4. 19-3007
5. 21-6666
6. 21-7783

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Total paid in 2021 was \$592,010 for 18.17 square miles of coverage. These fees encompass all services ShotSpotter currently provides to Oakland. There are no additional charges for meetings, reports, analysis and training. These funds come from OPD's General Purpose Fund.

- K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for policy changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

For any questions with this report, please contact Trevelyan Jones, Captain, OPD, Ceasefire Section, at tjones@oaklandca.gov

Respectfully submitted,

Trevelyan Jones

Trevelyan Jones, Captain, OPD, Ceasefire Section

Reviewed by,
Drennon Lindsey,
Deputy Chief, Bureau of Investigations

Paul Figueroa, Captain
OPD, Criminal Investigations Division

Carlo Beckman, Police Services Manager
OPD, Research and Planning Section

Prepared by:
Bruce Stoffmacher, Privacy and Legislation Manager
OPD, Bureau of Services

Attachment A - Shot Spotter Coverage Areas

Phase I with red borders (Activated in 2006): 6.2 square miles

East Oakland: East of High Street to 106th Avenue

West Oakland: East of Highway 980 to Frontage Road

Phase II with blue borders (Activated in 2013): 6.4 square miles

East Oakland: West of High Street to Park Boulevard

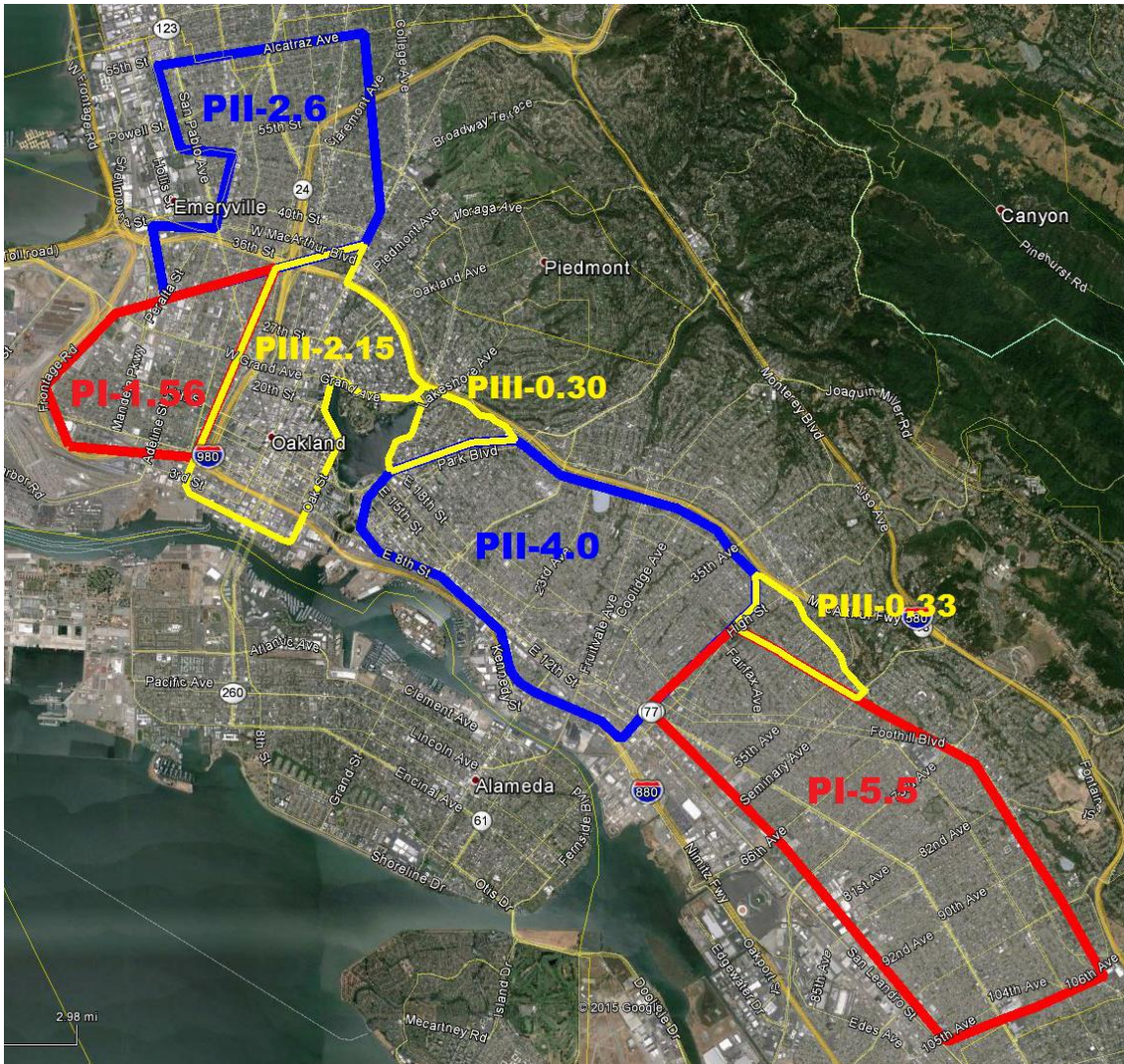
North Oakland: North of Highway 580 to Alcatraz Avenue

Phase III with yellow borders (Activated in 2016): 2.78 square miles

Downtown Oakland: Jack London Square to about West MacArthur Boulevard

Cleveland Height area: East of Lake Merritt to Highway 580 & Park Boulevard

Maxwell Park: East of High Street to Highway 580 & Mills College







MEMORANDUM

TO: LeRonne Armstrong,
Chief of Police

FROM: Drennon Lindsey, Deputy Chief of Police
OPD, Bureau of Investigations

SUBJECT: Unmanned Aerial System (UAS
or Drone) – 2021 Annual Report

DATE: March 9, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology “Oversight following City Council approval” requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

The PAC voted unanimously to recommend City Council adoption of OPD’s Departmental General Order (DGO) I-25: Unmanned Aerial System (UAS) Use Policy on May 14, 2020. The City Council adopted Resolution No. 88454 C.M.S. which approved OPD’s DGO I-25. OMC 9.64.040 requires that, after City Council approval, OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council.

Lieutenant Daza-Quiroz is currently the UAS Program Coordinator.

2021 Data Points

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

From the “Surveillance Impact Use Report for the Unmanned Aerial System (UAS)”

An Unmanned Aerial System (UAS) is an unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV)), and all of the supporting or attached components designed for gathering information through imaging, recording, or any other means.

*UAS are controlled from a remote-control unit (similar to a tablet computer).
Wireless connectivity lets pilots view the UAV its surroundings from a birds-eye*

perspective. UAV pilots can leverage control unit applications to pre-program specific GPS coordinates and create an automated flight path for the drone.

UAS have cameras so the UAS pilot can view the aerial perspective. UAS proposed for use by OPD and/or the Alameda County Sheriff's Office use secure digital (SD) memory cards to record image and video data; SD cards can be removed from UAS after flights to input into a computer for evidence.

UAS technology was used in the following ways/with the following outcomes in 2021:

Fifty-One (52) uses. Currently, OPD has no ownership of UAS's. All deployments and missions are conducted by the Alameda County Sheriff's Office (ACSO) or neighboring agencies with UAS Programs. In 2021, ACSO, and San Leandro Police Department (SLPD) responded to OPD requests. ACSO at times monitors radio channels and will respond prior to being requested¹. However, all agencies will only deploy if requested by an OPD commander and if policy requirements are met. OPD ESU has created a spreadsheet to track and monitor outside agency deployments. Lt. O. Daza-Quiroz sent a department wide email mandating all commanders who deploy drones to author documentation, similar to the protocol for use of the Emergency Rescue / Armored Vehicles. This process has allowed for appropriate documentation.

Table 1 below details the deployments of ACSO Drones in 2021 in the City of Oakland

Table 1: 2021 ACSO OPD Drone Deployments

Incident Type	Number
Mass casualty incidents	0
Disaster management	0
Missing or lost persons	3
Hazardous material releases	1
Sideshow events	4
Rescue operations	1
Training	0
Barricaded suspects	13
Hostage situations	0
Armed suicidal persons	1
Arrest of armed and/or dangerous persons	21
Scene documentation for evidentiary or investigation value	7
Operational pre-planning	1
Service of high-risk search and arrest warrants	0
Exigent circumstances	0
Total	52

Additionally, there were six incidents where ACSO responded and did not deploy. Reasons noted for these 'non-deployments were: inclement weather and suspect(s) already detained prior to arrival.

¹ ACSO has access to OPD radio channels and can monitor; ACSO personnel at times can respond to a call for service.

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

(52) Fifty-Two. Outside Law Enforcement Agencies have access to UAS technology, and both provides OPD with the recordings and stores the information in their logs per their respective policy requirements.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The technology was never installed upon fixed objects.

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year

Table 2 below details the Police Areas where UAS were deployed in 2021.

Table 2: OPD UAS Deployment by Police Area

Deployment by Area	Total Deployments
Area 1	9
Area 2	5
Area 3	9
Area 4	8
Area 5	17
Citywide	4*
Total*	52

** There were four deployments for Sideshow which were not documented as a specific area; the sideshow activity involved moving vehicles and involved multiple police areas.*

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

Table 3 below provides race data related to 2021 UAS deployments.

Table 3: Race of Detainees Connected to OPD UAS Deployments in 2021

	Race – Female	Race - Male	Total
Black	2	18	20
Hispanic	0	5	5
Asian	2	1	3
White	1	1	2
Other	0	1	1
Total			31

OPD knows the race of detainees connected to UAS deployments. However, the race of individuals involved in many UAS deployments is not known. There are cases such as barricaded suspects, where no suspect is ever discovered or detained. There could also be UAS uses for missing persons where the person's identity is not entirely known nor discovered.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information

The OPD Electronic Surveillance Unit (ESU) maintained a list of all UAS deployment logs for record and tracking purposes. This list was reviewed periodically for accuracy and for assessment of any policy violations. All OPD commanders were directed to send communications to ESU for any UAS request or use – similar to OPD protocols for use of Emergency Rescue / Armored Vehicles. No policy violations were found, and no corrective actions were warranted nor needed in 2021.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

OPD is not aware of any data breaches; ACSO has confirmed that they have not discovered any data breaches

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Table 4 below provides 2021 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2021 year. UAS deployments connect to this citywide data in several ways. For example, barricaded suspect incidents are related to several types of crimes listed below. Similarly, arrest of

armed and dangerous suspects, and crime scene documentation also relate to this citywide crime data.

Table 4: 2021 OPD Type 1 Crime Data

Part 1 Crimes <i>All totals include attempts except homicides</i>	01-01-2020 through 12-31-2020	01-01-2021 through 12-31-2021	Year-to-Date % Change 2020 vs. 2021	3-Year Year-to-Date Average	YTD 2021 vs. 3-Year YTD Average
Homicide - 187(a)	102	124	22%	100	24%
• Homicide - all other *	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• With Firearm	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• Auto	6,221	8,179	31%	8,921	-8%
• Residential	1,247	1,055	-15%	1,370	-23%
• Commercial	958	670	-30%	750	-11%
• Other/Unknown	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

- I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates.

There were two public records requests (PRR) opened in 2020 that have not been closed as of December 31, 2021, relating to drones:

- 20-3056; and
- 20-6466.

OPD's Records Division is still processing these two PRRs in 2021 and into 2022 because the full information request in each case is very broad and extends beyond the one technology or specific uses.

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year

(\$0.00) Zero. OPD did not incur any maintenance, licensing, or training costs.

- K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

No requests for policy changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Reviewed by,
Jeff Thomason, Lieutenant
OPD, Support Operations Section

Prepared by:
Omar Daza Quiroz, Lieutenant
OPD, Electronic Support Unit (ESU)

Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Unit



MEMORANDUM

TO: LeRonne Armstrong,
Chief of Police

FROM: Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

SUBJECT: Live stream transmitter– 2021
Annual Report

DATE: March 15, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology “Oversight following City Council approval” requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Oakland Police Department (OPD) I-23: Live Stream Transmitter Use Policy governs OPD’s use of Live Stream Transmitters; the policy was approved by the City Council on April 21, 2020 through Resolution No. 88099 C.M.S., as well as OMC 9.64.040, requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council. The information provided below is compliant with the annual report policy requirements of OMC 9.64.040 and DGO I-23.

Sergeant Inez Ramirez is currently the Live Stream / Video Team Program Coordinator.

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

*OPD used the livestream transmitter technology one time in 2021. **Attachment A** to this report provides the detail from the required after-action report provided to the City’s Privacy Advisory Commission (PAC) as well as the City’s Chief Privacy Officer. From page one of the report:*

“The City of Oakland activated its Emergency Operations Center (EOC) on May 1, 2021 and, as part of the City’s Incident Command System response, OPD staffed the EOC positions therein including the role of OPD Operations Incident Command. The activation and associated operations were necessitated by the plan to address planned but unpermitted crowd management events associated to “May Day” parades, marches, rallies, demonstrations, protests and May 1st events. Although OPD deployed video teams with EOC video stream transmitters during the entire operational period, the technology use was

Privacy Advisory Commission
April 7, 2022

limited to evening and late evening hours to better assess, plan, direct, and respond to circumstances associated with a march of approximately 70 persons.”

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

DGO I-11 does provide that OPD may share live stream data with other law enforcement agencies that have a right to know and a need to know¹, such as an inspector with the District Attorney’s Office. However, no live stream data was downloaded, retained, or shared with different agencies. Video was streamed into the EOC/DOC. Any supporting agency inside the EOC would have viewed the live stream. No live stream video was saved/downloaded at the EOC/DOC. No live stream video was shared with other law enforcement agency, unless they viewed it live on the screen at the EOC/DOC. No one is allowed at the EOC without:

- 1. Authorization*
- 2. Verification of their status, department, rank, and title*
- 3. All verifications are documented by OPD and or City Administration.*

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The transmitters are attached to video cameras which are handheld by officers monitoring the events.

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

The live stream transmitters were deployed in areas where the protests and marches occurred in parts of downtown Oakland.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology’s adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology’s use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology’s impact on privacy interests is outweighed by the City’s administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

¹ DGO I-23 explains that a right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

OPD did notify the City's Chief Privacy Officer and Chair and Co-Chair of the Privacy Advisory Commission on May 3, 2021 of the use of the equipment on May 1, 2021. The report was discussed at the public May 5, 2021 PAC meeting.

In terms of an "analysis shall also identify the race of each person that was subject to the technology's use:"

- *data was not generated from use of the livestream transmitter as the transmission was not recorded; there is no data to analyze.*
- *Additionally, the technology is used to survey a large area for situational awareness. The administration burden would be high and challenging to determine the race of everyone who may have been streamed via the live video during even one usage over the course of an hour or more in an event with hundreds of people.*

For the reasons cited above, staff recommends that the PAC waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by both the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

The one use in 2021 was reviewed for adherence to policy and internal protocols:

- *Video was not recorded during the incident (see **Attachment A** for full report);*
- *Appropriate staff were notified of use and the City's Privacy Officer and PAC were notified according to policy.*
- *Technology was properly stored with the OPD Information Technology Unit (ITU).*
- *OPD is not aware of any policy violations from use of the live stream transmitters in 2021.*

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

OPD is not aware of any data breaches; furthermore, data was not generated from use of the livestream transmitter as the transmission was not recorded.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

*The "Report on Video Stream Request and Usage," dated May 3, 201 (see **Attachment A**) explains that the decision to activate live stream and recording during the evening hours:*

- *Video Team assignments and equipment are a recommended if not required component of OPD response to planned events involving potentially large crowds.*
- *Live stream may be authorized by the Incident Commander.*
- *The march was reportedly organized or promoted by the same source linked to a April 16, 2021 march that resulted in numerous instances of property damage, arson, assault, and battery of police officers; the apparent organizers or participants of that event had refused to communicate with or otherwise cooperate with police*
- *The imagery used to promote the unpermitted march displayed burning structures with proximate protest activity inferring desired crimes of arson.*
- *The text used in this event's main social media/internet posting urged absences of livestreaming, picture taking, and "snitching" for an inferred intent to commit criminal acts with reduced chances of being identified and arrested.*
- *The text used in this event's main social media/internet posting was inherently anti-police and requested participants to "bring soup." Soup cans were thrown at officers with intent to injure during past anti-police demonstrations including the previously referenced 16 Apr 21 event.*
- *Open media sources had reported "antifa" communication and meetings in nearby Northern Ca communities identifying "May Day" as an opportunity to "kill cops." Persons affiliated with the "antifa" group(s) had ties to past Oakland events in which violence was used.*
- *The social media/internet posting urged persons to wear all black. "Black Blok" is a tactic in which persons desiring to commit unlawful acts wear black clothing so that they may not be easily identified or found within the crowd during or after committing criminal acts.*
- *The vast majority of persons assembled at Frank Ogawa Plaza arrived wearing all black.*
- *Many persons arriving at Frank Ogawa Plaza possessed bulky backpacks. Backpacks have been used to secret "tools of violence" and other instruments to damage property, commit acts of arson, or batter police officers.*
- *Officers observed a bag of canned soup brought to or possessed by persons assembling at Frank Ogawa Plaza.*
- *Attempts to communicate with the persons assembled in Frank Ogawa Plaza failed to achieve cooperation in establishing a march route, police liaison, and means by which criminal activity could be mitigated or otherwise cooperatively addressed.*
- *When persons assembled at Frank Ogawa Plaza entered the roadway with apparent intent to march, I authorized live stream and recording in order to better observe, plan, direct, and assess the crowd control incident in best effort to prevent, record, and address instances of property damage, arson, crime, and assaultive behavior.*

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There were no PRRs related to live stream transmitters in 2021.

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

One hundred thirty thousand dollars (\$130,000) in one-time purchase cost. In 2021, OPD upgraded the video streaming system that was originally purchased in 2011. This included camera equipment, transmitters, receivers and software licensing.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Reviewed by,
Jeffrey Thomason, Lieutenant
OPD, Special Operations Section

Prepared by:
David Pullen, Officer
OPD, Bureau of Services, Information Technology Unit

Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Unit

Attachments (1)
Appendix A: 2020 Video Stream Deployment Memos

CITY OF OAKLAND

Memorandum

TO: Privacy Advisory Commission and Chief Privacy Officer
FROM: Christopher Bolton, Deputy Chief of Police
DATE: May 3, 2021
RE: Report on Video Stream Request and Usage

This Memorandum summarizes the use of live-stream transmitters by the Oakland Police Department (OPD) in support of the specified event. This memorandum is provided in accordance with OPD Department General Order I-23: “Handheld Livestream Transmitter¹.”

Purpose (from DGO I-23)

Live stream camera transmitters allow OPD to deploy a minimal level of police presence while providing critical situational awareness to OPD commanders. A small number of officers can monitor events and provide real-time footage to Command. This information helps OPD Command to make efficient deployment decisions.

OPD commanders need real time situational awareness to ensure public safety in public spaces. Real-time information regarding events (e.g., crowd management facilitation, coordinated response to catastrophic unplanned events) provides critical information for OPD commanders when making resource deployment decisions. Authorized personnel utilizing cameras with live-streaming transmitters can provide important situational awareness to OPD without the need to deploy many officers.

Livestream Transmitter Use

The City of Oakland activated its Emergency Operations Center (EOC) on May 1, 2021 and, as part of the City’s Incident Command System response, OPD staffed the EOC positions therein including the role of OPD Operations Incident Command. The activation and associated operations were necessitated by the plan to address planned but unpermitted crowd management events associated to “May Day” parades, marches, rallies, demonstrations, protests and May 1st events. Although OPD deployed video teams with EOC video stream transmitters during the entire operational period, the technology use was limited to evening and late evening hours to better assess, plan, direct, and respond to circumstances associated with a march of approximately 70 persons. As the

¹ DGO I-23: Sec. III.B “Restricted Use,” Sec 4.ii: ii. For each use of live stream transmitters, OPD shall articulate the facts and circumstances surrounding the use in a written statement filed with the Chief Privacy Officer and/or Chair of the Privacy Advisory Commission within 72 hours. This statement (and the use itself) shall be included in the required Annual Report.

Incident Commander, my decision to utilize video teams with streaming and recording² capabilities was based on numerous factors but driven by an overriding desire and mandate to videotape in a manner that minimizes interference with people lawfully participating in First Amendment activities. As evidence of this commitment, video stream was not utilized to record or display the actions of more than 150 persons during the peaceful car caravan and march early within the day. The below is a non-inclusive list of factors informing my decision to activate live stream and recording during the evening hours:

- Video Team assignments and equipment are a recommended if not required component of OPD response to planned events involving potentially large crowds.
- Live stream may be authorized by the Incident Commander.
- The march was reportedly organized or promoted by the same source linked to a April 16, 2021 march that resulted in numerous instances of property damage, arson, assault, and battery of police officers; the apparent organizers or participants of that event had refused to communicate with or otherwise cooperate with police/
- The imagery used to promote the unpermitted march displayed burning structures with proximate protest activity inferring desired crimes of arson.
- The text used in this event's main social media/internet posting urged absences of livestreaming, picture taking, and "snitching" for an inferred intent to commit criminal acts with reduced chances of being identified and arrested.
- The text used in this event's main social media/internet posting was inherently anti-police and requested participants to "bring soup." Soup cans were thrown at officers with intent to injure during past anti-police demonstrations including the previously referenced 16 Apr 21 event.
- Open media sources had reported "antifa" communication and meetings in nearby Northern Ca communities identifying "May Day" as an opportunity to "kill cops." Persons affiliated with the "antifa" group(s) had ties to past Oakland events in which violence was used.
- The social media/internet posting urged persons to wear all black. "Black Blok" is a tactic in which persons desiring to commit unlawful acts wear black clothing so that they may not be easily identified or found within the crowd during or after committing criminal acts.
- The vast majority of persons assembled at Frank Ogawa Plaza arrived wearing all black.
- Many persons arriving at Frank Ogawa Plaza possessed bulky backpacks. Backpacks have been used to secret "tools of violence" and other instruments to damage property, commit acts of arson, or batter police officers.

² In accordance with DGO I-23, IV.B Livestream Camera Data, "Retention,": Handheld live stream cameras can send the digital stream wirelessly. The EOC does not record this data; data recorded by the handheld cameras is maintained by the OPD IT Unit within in the Bureau of Services (BOS). Personnel using live-stream cameras shall return them at the end of their shift to the IT Unit. For data that is captured and used as evidence, such data shall be turned in and stored as evidence pursuant to existing policy. Otherwise, camera data will be destroyed after 30 days.

- Officers observed a bag of canned soup brought to or possessed by persons assembling at Frank Ogawa Plaza.
- Attempts to communicate with the persons assembled in Frank Ogawa Plaza failed to achieve cooperation in establishing a march route, police liaison, and means by which criminal activity could be mitigated or otherwise cooperatively addressed.
- When persons assembled at Frank Ogawa Plaza entered the roadway with apparent intent to march, I authorized live stream and recording in order to better observe, plan, direct, and assess the crowd control incident in best effort to prevent, record, and address instances of property damage, arson, crime, and assaultive behavior.

RD# or Incident #: 21- 019659

Date of Incident: 1 May 21

Type of Event: Protest

Was EOC/DOC activated: YES

Number of Video Streams provide to EOC/DOC: 3 video streams.

Initial Request: Video Teams were requested by D.C. C. Bolton on 28 Apr 21.

Summary: On 1 May 21 at 2045 hrs. at the direction of D.C. C. Bolton, three video streams were provided by the Video Team to the EOC. The livestream ended at approximately 2230 hrs, when the demonstration ended.

Ann Pierce
Sergeant of Police
Bureau of Investigations
Oakland Police Department

Bruce Stoffmacher
Legislation and Privacy Manager
Research and Planning Section
Oakland Police Department

Oakland Police Department

Criminalistics Laboratory

Requests Completed Between 01 Jan 21 and 31 Dec 21

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
01036278	17022	Sex Offense	1	EK	09/15/20	03/29/21	05/13/21	
01063412	17023	Sex Offense	1	EK	09/15/20	03/29/21	05/20/21	
02001819	17024	Rape	1	EK	09/16/20	03/29/21	05/20/21	
02043259	17025	Rape	1	EK	09/16/20	03/30/21	05/19/21	
02050483	17026	Rape	1	HW	09/16/20	03/30/21	05/20/21	
07026094	5128	Homicide	6	BC	12/08/20	12/09/20	01/14/21	
10023028	6974	Rape	3	CAG	10/14/21	10/22/21	12/30/21	
16031898	10693	Homicide	2	RJ	02/11/21	03/31/21	05/17/21	
16064685	11244	Homicide	4	CAG	04/21/21	04/21/21	05/07/21	
18023529	14166	SC Unexplained Death	3	AL	05/31/18	02/11/21	03/19/21	
18027499	12784	Rape	2	CAG	12/14/20	12/29/20	03/01/21	
18027646	17020	Robbery	2	EK	07/19/18	03/31/21	05/20/21	
18031763	12852	Assault	4	EK	06/28/18	03/31/21	05/20/21	
18033728	17021	Assault	2	NYN	07/11/18	04/01/21	05/20/21	
			3	NYN	08/03/18	04/01/21	05/20/21	
18038487	14949	Weapons	2	EK	08/09/18	03/31/21	05/19/21	
18042053	17058	Carjacking	1	RJ	10/11/18	03/31/21	05/24/21	
18043786	17059	Weapons	2	RJ	08/31/18	03/31/21	06/01/21	
18044586	15313	Robbery	2	SF	09/07/18	06/03/20	10/06/21	
18046211	17060	Other Criminal	4	SF	09/14/18	03/31/21	07/19/21	
18053409	13246	Assault	2	EK	03/07/19	03/31/21	04/29/21	
18055776	13318	Rape	3	HW	04/21/21	04/30/21	05/19/21	
18057757	13520	Homicide	16	HW	12/14/20	01/04/21	01/19/21	
18058849	17061	Robbery	2	SF	11/26/18	03/31/21	07/16/21	
18059648	13383	Homicide	5	RJ	12/06/18	10/29/20	01/29/21	
			7	RJ	12/10/18	10/29/20	01/29/21	
18059725	15124	Robbery	3	HW	11/29/18	02/22/21	05/19/21	
18060226	13421	Weapons	2	RJ	12/18/18	03/31/21	05/11/21	
19000506	13844	Assault	3	EK	07/29/19	05/21/21	10/13/21	
19002000	13664	Robbery	2	VSS	02/14/19	11/24/20	02/02/21	
19003036	17770	Weapons	2	AL	01/25/19	07/28/21	10/11/21	
19003137	13656	Rape	2	HW	01/15/21	01/19/21	02/10/21	
19006349	13634	Assault	3	SF	04/02/21	06/28/21	09/22/21	
19008265	17103	Assault	3	EK	02/25/19	04/05/21	04/29/21	

Attachment A: OPD Forensic DNA 2021 Annual Report

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
19010466	13706	Assault	2	SF	03/12/19	06/28/21	09/21/21	
19012016	17438	Robbery	4	NYN	03/14/19	05/21/21	08/06/21	
19016757	17340	Weapons	2	AL	04/05/19	05/06/21	06/15/21	
19019197	18017	Robbery	1	VSS	01/21/20	07/13/21	11/19/21	
19022636	14058	Weapons	1	RJ	05/07/19	03/31/21	05/18/21	
19023505	13988	Assault	3	EK	05/15/19	03/30/21	04/29/21	
19028136	17062	Weapons	3	EK	06/07/19	03/31/21	05/11/21	
19029659	17339	Robbery	2	AL	07/08/19	05/06/21	06/15/21	
19030801	17119	Weapons	4	EK	06/20/19	04/06/21	04/29/21	
19034391	14163	Assault	5	EK	07/09/19	03/30/21	04/29/21	
19037014	17846	Robbery	1	SF	07/31/19	08/10/21	10/18/21	
19038175	14227	Assault	3	EK	07/30/19	04/01/21	05/11/21	
19038270	17342	Carjacking	3	EK	07/30/19	05/12/21	06/14/21	
19039295	14221	Assault	2	CAG	08/08/19	04/29/21	07/29/21	
19040045	14953	Homicide	6	HW	02/03/21	02/03/21	04/05/21	
19042455	17290	Burglary	1	CAG	08/26/19	04/30/21	08/11/21	
19042647	16239	Weapons	2	CAG	08/20/19	10/21/20	01/11/21	
19043099	17094	Burglary	2	NYN	08/29/19	04/02/21	05/03/21	
19054375	14447	Robbery	3	EK	03/18/21	08/10/21	11/01/21	
19054399	17343	Sex Offense	1	EK	09/30/19	05/10/21	05/26/21	
19055593	17847	Weapons	1	EK	03/17/21	08/10/21	11/01/21	
19057039	16421	Burglary	1	RJ	11/05/19	11/24/20	01/15/21	
19057574	14479	Assault	2	VSS	11/08/19	03/12/21	04/15/21	
19058068	14485	Assault	1	VSS	11/07/19	03/12/21	04/15/21	
19058600	14504	Homicide	8	CAG	11/19/19	07/23/21	08/11/21	
19058976	15984	Homicide	3	CAG	11/14/19	03/15/21	05/12/21	
19059950	15985	Auto Theft	3	AL	11/21/19	06/07/21	07/09/21	
19060095	14541	Assault	3	AL	04/21/20	06/14/21	07/21/21	
19061640	16420	Robbery	1	VSS	11/26/19	11/24/20	02/08/21	
19062872	16619	Assault	1	AL	12/05/19	12/28/20	02/02/21	
19062955	15400	Weapons	2	SF	12/26/19	04/28/21	07/26/21	
19064132	17848	Robbery	2	HW	12/13/19	08/10/21	10/08/21	
19065714	14686	Rape	2	HW	01/27/21	02/04/21	03/17/21	
19065941	16896	Weapons	1	SF	12/23/19	03/01/21	05/20/21	
19066709	14997	Homicide	2	BC	09/29/21	10/06/21	12/08/21	
19067532	16897	Burglary	1	HW	01/21/20	02/24/21	04/26/21	
20000169	17631	Burglary	1	EK	01/21/20	07/06/21	08/10/21	
20000444	16354	Weapons	4	SF	03/10/21	07/07/21	10/07/21	
20000448	17070	Weapons	1	NYN	01/15/20	03/31/21	05/03/21	

Attachment A: OPD Forensic DNA 2021 Annual Report

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
20000449	17148	Weapons	1	NYN	01/15/20	04/09/21	05/11/21	
20000555	17632	Burglary	1	SF	01/15/20	07/07/21	10/04/21	
20001193	17633	Robbery	1	SF	01/21/20	07/07/21	09/13/21	
20002337	17808	Robbery	1	AL	01/14/20	08/26/21	10/11/21	
20002670	14720	Assault	2	AL	01/16/20	08/26/21	10/11/21	
20003256	17856	Burglary	1	SF	01/27/20	08/06/21	10/11/21	
20003406	14910	Hit and Run	2	VSS	04/13/21	04/20/21	05/17/21	
20003526	17849	Assault	3	EK	01/22/20	08/10/21	10/08/21	
20005624	17920	Burglary	1	EK	02/20/20	08/19/21	10/15/21	
20005838	15204	Rape	3	HW	12/23/20	02/18/21	03/10/21	
20010157	15327	Rape	3	AL	10/13/20	10/19/20	01/14/21	
20011135	17921	Assault	2	SF	03/06/20	08/18/21	12/03/21	
20011754	17079	Robbery	1	EK	08/17/20	04/01/21	04/29/21	
20012506	14850	Weapons	3	EK	03/30/20	04/01/21	04/29/21	
20013312	16355	Robbery	1	RJ	04/15/20	11/10/20	02/19/21	
20014597	17086	Assault	1	EK	03/26/20	04/05/21	05/13/21	
20014820	17380	Homicide	1	AL	05/10/21	05/24/21	07/13/21	
20016868	15010	Weapons	2	SF	03/31/20	05/19/21	07/26/21	
20018666	15160	Assault	1	NYN	04/17/20	05/26/21	08/12/21	
20019001	15279	Homicide	3	SF	04/28/20	08/31/20	04/22/21	
20019026	15926	Robbery	1	SF	04/15/20	08/31/20	03/24/21	
20019050	16512	Weapons	2	HW	04/30/20	12/11/20	01/04/21	
20019088	15110	Assault	3	AL	04/16/20	03/24/21	05/27/21	
20019684	15478	Rape	2	HW	06/16/20	10/27/20	01/04/21	
20019806	16683	Weapons	2	HW	01/19/21	02/16/21	03/19/21	
20020312	15139	Homicide	3	CAG	04/24/20	09/01/21	12/06/21	
20020603	15229	Weapons	2	NYN	05/11/20	05/26/21	07/26/21	
20020660	15140	Weapons	2	SF	04/24/20	09/08/21	11/18/21	
20021531	15173	Assault	3	NYN	04/30/20	03/30/21	05/14/21	
20022305	15332	Sex Offense	2	CAG	05/28/20	11/09/20	03/03/21	
20022757	16881	Carjacking	2	CAG	05/26/20	06/09/21	09/23/21	
20023314	16401	Carjacking	2	VSS	09/23/20	11/19/20	02/19/21	
20025235	17344	Weapons	1	EK	05/26/20	05/10/21	06/14/21	
20025284	15927	Burglary	3	SF	10/19/20	12/07/20	02/09/21	
20026062	17056	Robbery	1	NYN	05/28/20	03/31/21	05/20/21	
20026824	15672	Homicide	3	HW	07/27/20	11/23/20	01/26/21	
20028070	16228	Rape	1	RJ	10/14/20	10/19/20	01/24/21	
20029650	15441	Homicide	3	SF	07/06/20	06/28/21	09/08/21	
20029732	15414	Other Person	1	VSS	06/22/20	07/03/20	02/16/21	

Attachment A: OPD Forensic DNA 2021 Annual Report

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
20030227	15803	Rape	1	SF	08/04/20	08/11/20	05/21/21	
20031564	17012	Carjacking	1	VSS	07/22/20	03/25/21	05/13/21	
20033467	16423	Robbery	2	VSS	07/09/20	11/24/20	02/11/21	
20034591	17418	Assault	3	SF	07/16/20	05/18/21	07/23/21	
20035047	15922	Homicide	3	HW	12/07/20	02/16/21	03/19/21	
20035129	17533	Robbery	2	AL	07/22/20	06/14/21	09/02/21	
20035334	15665	Assault	4	HW	07/21/20	09/17/20	01/06/21	
20035880	15859	Sex Offense	2	HW	07/23/20	10/27/20	01/15/21	
20036082	17527	Weapons	2	CAG	07/24/20	06/09/21	09/20/21	
20037924	16164	Homicide	1	AL	08/05/20	10/05/20	01/20/21	
20038059	17439	Assault	2	CAG	08/04/20	05/24/21	08/19/21	
20038267	15801	Sex Offense	1	VSS	08/05/20	08/11/20	01/15/21	
20038278	15856	Sex Offense	3	HW	01/25/21	01/27/21	03/17/21	
20038696	15879	Attempted Murder	3	AL	11/12/21	12/13/21	12/17/21	
20038766	16403	Attempted Murder	1	HW	10/19/20	11/23/20	01/25/21	
20039000	16296	Robbery	1	RJ	09/03/20	10/29/20	01/04/21	
20039247	15855	Rape	1	SF	08/10/20	08/17/20	01/06/21	
20039558	16231	Rape	1	AL	10/14/20	10/19/20	01/08/21	
			2	HW	10/14/20	11/24/20	01/29/21	
20040117	16425	Assault	1	CAG	08/24/20	11/24/20	03/04/21	
20040194	15972	Rape	1	VSS	09/01/20	09/10/20	05/14/21	
20040600	15920	Weapons	3	SF	09/14/20	12/07/20	04/13/21	
20041076	16404	Rape	1	HW	11/19/20	11/24/20	03/10/21	
20041152	16269	Rape	1	CAG	10/16/20	10/28/20	04/02/21	
20041255	15907	Weapons	2	RJ	08/24/20	03/23/21	06/30/21	
20041382	16298	Sex Offense	1	RJ	10/27/20	10/29/20	02/11/21	
20041824	16165	Assault	1	CAG	09/15/20	10/05/20	01/28/21	
20042634	15993	Rape	1	SF	09/03/20	09/15/20	01/15/21	
			2	SF	07/15/21	07/22/21	10/08/21	
20043707	15967	Attempted Murder	2	SF	09/10/20	12/07/20	03/24/21	
20043942	15995	Rape	1	SF	09/08/20	09/15/20	03/19/21	
20043956	15983	Assault	2	CAG	09/08/20	11/12/20	01/22/21	
20044529	16144	Rape	1	CAG	09/29/20	10/05/20	01/06/21	
20044704	16229	Assault	1	AL	10/14/20	10/19/20	01/08/21	
20045598	17345	Weapons	3	AL	12/10/20	06/15/21	07/27/21	
20045789	16074	Assault	3	HW	09/24/20	11/24/20	02/22/21	
20046588	16153	Rape	1	AL	09/25/20	10/12/20	01/08/21	
20046726	16230	Rape	1	AL	10/14/20	10/19/20	01/20/21	
20047237	16154	Rape	1	HW	09/30/20	10/12/20	01/15/21	

Attachment A: OPD Forensic DNA 2021 Annual Report

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
20047624	16126	Robbery	2	HW	10/19/20	10/27/20	01/06/21	
20047706	16388	Homicide	3	VSS	10/21/20	11/17/20	02/08/21	
20047859	16299	Rape	1	CAG	10/27/20	10/29/20	01/06/21	
20047977	16271	Rape	1	HW	10/21/20	10/28/20	02/08/21	
20048007	16272	Homicide	4	SF	09/01/21	09/27/21	12/13/21	
20048034	16405	Attempted Murder	1	HW	09/22/20	11/24/20	01/29/21	
20048227	16241	Homicide	3	RJ	10/19/20	11/17/20	02/08/21	
20048319	16204	Homicide	1	VSS	10/05/20	10/13/20	02/09/21	
20048495	16422	Assault	1	CAG	10/02/20	11/24/20	02/10/21	
20048886	16291	Assault	2	CAG	10/15/20	11/10/20	01/22/21	
20048907	16202	Homicide	4	VSS	10/26/20	01/15/21	01/27/21	
			6	VSS	11/23/20	12/17/20	01/19/21	
20049373	17742	Homicide	2	AL	10/13/20	07/26/21	10/01/21	
20049517	16337	Rape	1	SF	11/04/20	11/09/20	01/06/21	
20049588	16301	Rape	1	CAG	10/27/20	10/29/20	03/29/21	
20049971	16365	Assault	1	RJ	11/03/20	11/12/20	03/19/21	
20050051	16275	Rape	1	HW	10/14/20	10/28/20	01/04/21	
			2	HW	10/14/20	11/24/20	01/04/21	
20050187	16302	Other Person	1	RJ	10/27/20	10/29/20	01/15/21	
			2	RJ	06/09/21	06/09/21	07/16/21	
20050314	16276	Rape	1	HW	10/21/20	10/28/20	01/08/21	
20050759	16419	Homicide	1	RJ	10/29/20	11/24/20	02/08/21	
20050946	16338	Rape	1	RJ	11/05/20	11/09/20	01/29/21	
20050969	16294	Homicide	3	HW	10/21/20	12/09/20	02/26/21	
			6	HW	11/16/20	08/11/21	10/08/21	
			7	HW	01/04/21	01/05/21	02/26/21	
20051169	16432	Assault	4	NYN	11/12/20	06/18/21	08/12/21	
20051358	16250	Assault	2	CAG	10/21/20	11/24/20	03/04/21	
20051397	16554	Homicide	2	SF	11/16/20	12/15/20	02/11/21	
20051805	16321	Assault	3	CAG	11/16/20	02/04/21	03/24/21	
20051860	16681	Sex Offense	1	RJ	01/05/21	01/08/21	03/01/21	
			2	HW	01/05/21	02/18/21	03/29/21	
20052507	16406	Homicide	3	HW	11/03/20	11/24/20	02/08/21	
20052551	16326	Assault	2	CAG	11/02/20	12/07/20	03/01/21	
20052825	16627	Homicide	1	HW	12/28/20	01/05/21	02/10/21	
20052863	16339	Rape	1	SF	10/28/20	11/09/20	01/06/21	
			2	CAG	10/28/20	01/19/21	05/11/21	
20052901	16409	Homicide	2	VSS	10/29/20	11/20/20	01/25/21	
20053306	16581	Rape	1	CAG	12/09/20	12/21/20	03/22/21	

Attachment A: OPD Forensic DNA 2021 Annual Report

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
20053392	17011	Robbery	3	VSS	11/09/20	03/25/21	05/07/21	
20053459	16398	Rape	1	RJ	11/12/20	11/18/20	01/29/21	
20053480	16767	Homicide	2	CAG	11/19/20	02/01/21	04/19/21	
20053606	16659	Rape	1	RJ	12/23/20	01/08/21	03/01/21	
20053624	16370	Homicide	3	NYN	02/24/21	03/31/21	05/14/21	
20053646	16596	Sex Offense	1	CAG	12/09/20	12/23/20	03/26/21	
20053666	16340	Sex Offense	1	SF	11/05/20	11/09/20	01/06/21	
			2	CAG	11/05/20	01/19/21	05/11/21	
20054210	17010	Homicide	2	AL	11/18/20	03/25/21	05/21/21	
20054745	16693	Homicide	4	HW	01/06/21	02/16/21	02/25/21	
20054927	16625	Sex Offense	1	AL	12/04/20	01/27/21	03/19/21	
20055028	18264	Homicide	1	CAG	11/16/20	10/19/21	12/15/21	
20055058	16399	Rape	2	RJ	11/12/20	11/19/20	01/14/21	
20055306	17923	Homicide	2	EK	03/19/21	08/18/21	10/15/21	
20055519	16395	Attempted Murder	2	HW	11/12/20	11/18/20	03/01/21	
20055785	16626	Sex Offense	1	AL	12/08/20	12/30/20	06/18/21	
20055980	16624	Rape	1	CAG	12/08/20	12/29/20	05/05/21	
20056351	16407	Rape	1	HW	11/18/20	11/25/20	02/16/21	
20056415	16490	Sex Offense	1	HW	12/04/20	12/07/20	02/04/21	
20056695	16868	Carjacking	2	HW	11/19/20	02/22/21	04/26/21	
20056752	16618	Assault	2	AL	11/19/20	12/28/20	02/10/21	
20056868	16555	Homicide	2	AL	11/23/20	01/11/21	02/02/21	
20057045	16556	Homicide	3	SF	11/23/20	12/16/20	01/19/21	
20057648	16491	Rape	1	HW	12/03/20	12/07/20	02/09/21	
20058685	16658	Robbery	2	HW	12/17/20	01/08/21	02/10/21	
20058691	16492	Rape	1	HW	12/03/20	12/07/20	02/19/21	
			3	HW	12/03/20	01/11/21	02/19/21	
20058808	16864	Attempted Murder	2	HW	12/09/20	02/22/21	04/26/21	
20059087	16571	Homicide	2	VSS	12/18/20	12/18/20	02/02/21	
20059088	16680	Rape	1	RJ	12/31/20	01/08/21	03/01/21	
20059133	16834	Homicide	1	HW	01/13/21	02/16/21	04/14/21	
			2	HW	01/29/21	02/16/21	04/14/21	
20059903	16553	Assault	1	AL	12/08/20	01/11/21	01/22/21	
20060041	16865	Hit and Run	1	AL	01/19/21	02/22/21	05/07/21	
20060055	16917	Homicide	6	HW	12/16/20	03/01/21	04/20/21	
			7	HW	12/17/20	03/01/21	04/20/21	
			8	HW	02/25/21	03/01/21	04/20/21	
			9	HW	12/17/20	08/18/21	08/31/21	
			11	HW	03/25/21	03/31/21	04/19/21	

Attachment A: OPD Forensic DNA 2021 Annual Report

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
20060158	17102	Weapons	2	NYN	12/10/20	04/02/21	05/03/21	
20060239	16642	Robbery	1	HW	12/23/20	01/06/21	02/09/21	
20060260	16660	Rape	1	HW	12/28/20	01/08/21	03/17/21	
20060346	17087	Assault	3	NYN	12/10/20	04/02/21	05/03/21	
20060412	17924	Assault	2	SF	03/19/21	08/18/21	12/03/21	
20060927	16662	Rape	1	AL	12/30/20	01/27/21	02/10/21	
20061418	16663	Rape	1	CAG	12/30/20	01/08/21	03/29/21	
			2	CAG	12/30/20	02/02/21	03/29/21	
20061565	16866	Homicide	3	HW	01/15/21	02/22/21	04/28/21	
20061583	16661	Rape	1	RJ	12/29/20	01/08/21	02/10/21	
20063716	17337	Assault	3	AL	01/06/21	05/06/21	06/15/21	
20063910	17346	Assault	3	AL	01/05/21	06/15/21	07/23/21	
200905	17288	Other Criminal	1	VSS	04/21/21	05/05/21	07/21/21	
			4	VSS	05/06/21	05/05/21	07/21/21	
21000009	16835	Homicide	3	HW	01/05/21	02/17/21	04/27/21	
			4	HW	02/09/21	02/17/21	04/27/21	
21000316	16691	Rape	1	SF	01/13/21	01/19/21	06/10/21	
21000541	17491	Weapons	3	SF	01/06/21	05/27/21	07/26/21	
21000730	16682	Sex Offense	1	RJ	01/06/21	01/08/21	03/01/21	
21000830	17634	Robbery	1	SF	03/31/21	07/07/21	10/13/21	
21000838	16667	Attempted Murder	1	HW	01/08/21	01/11/21	02/10/21	
			4	SF	03/31/21	07/07/21	09/23/21	
21000916	16845	Robbery	1	HW	02/11/21	02/17/21	03/17/21	
21001005	16698	Rape	1	SF	01/14/21	01/19/21	05/19/21	
21001493	17635	Homicide	1	EK	03/23/21	07/01/21	08/10/21	
21001658	16699	Rape	1	SF	01/14/21	01/19/21	03/19/21	
21001836	16739	Rape	1	VSS	01/21/21	01/27/21	04/12/21	
21002016	16738	Rape	1	VSS	01/19/21	01/27/21	04/14/21	
21002065	16826	Rape	1	AL	02/03/21	02/10/21	04/13/21	
21002412	16836	Homicide	1	HW	02/03/21	02/17/21	03/19/21	
21002569	16740	Homicide	1	VSS	01/21/21	01/27/21	03/17/21	
21002579	16846	Homicide	2	HW	02/09/21	02/17/21	03/19/21	
21002737	16793	Sex Offense	1	CAG	01/27/21	02/03/21	03/29/21	
21002740	16707	Homicide	1	HW	01/20/21	01/21/21	03/24/21	
21002803	16766	Rape	1	CAG	01/27/21	02/01/21	03/17/21	
21002982	16776	Sex Offense	1	CAG	01/28/21	02/02/21	05/11/21	
			2	CAG	06/15/21	06/15/21	09/02/21	
21003060	16825	Sex Offense	1	SF	01/29/21	02/10/21	04/12/21	
21003120	16757	Weapons	1	VSS	01/21/21	01/27/21	03/18/21	

Attachment A: OPD Forensic DNA 2021 Annual Report

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
21003728	16847	Weapons	2	HW	02/09/21	02/17/21	03/19/21	
21004076	17167	Assault	3	SF	02/08/21	04/13/21	06/22/21	
21004492	17168	Robbery	1	HW	02/03/21	04/13/21	06/09/21	
21005104	16824	Rape	1	SF	02/04/21	02/10/21	04/12/21	
21005639	16816	Weapons	4	NYN	02/16/21	03/30/21	05/14/21	
21005660	16863	Sex Offense	1	RJ	02/17/21	02/22/21	04/16/21	
21005856	16837	Rape	1	HW	02/09/21	02/18/21	04/14/21	
21007263	16985	Homicide	2	AL	03/16/21	03/25/21	05/10/21	
21007420	16999	Homicide	2	AL	03/12/21	05/07/21	08/10/21	
21007564	17169	Robbery	1	CAG	02/18/21	04/13/21	09/21/21	
21007594	17516	Weapons	2	CAG	03/29/21	09/03/21	12/13/21	
21007965	16961	Rape	1	VSS	03/04/21	03/09/21	04/30/21	
			2	VSS	04/06/21	04/07/21	05/07/21	
			3	VSS	07/20/21	07/20/21	09/08/21	
21008014	16960	Sex Offense	1	VSS	02/25/21	03/09/21	04/20/21	
21008066	16975	Sex Offense	1	CAG	03/10/21	03/15/21	06/28/21	
21008400	17347	Homicide	3	EK	03/01/21	05/12/21	06/15/21	
21008563	17000	Rape	1	AL	03/16/21	03/23/21	05/13/21	
21008884	17420	Homicide	3	SF	03/01/21	06/30/21	09/30/21	
21008893	17170	Homicide	2	HW	03/01/21	04/12/21	05/20/21	
21008933	16916	Homicide	1	SF	02/26/21	03/01/21	05/07/21	
			2	RJ	04/07/21	04/07/21	05/07/21	
			3	SF	04/27/21	04/27/21	05/07/21	
21009245	16986	Assault	1	CAG	03/10/21	03/15/21	06/25/21	
21009400	16976	Sex Offense	1	CAG	03/09/21	03/15/21	05/24/21	
21010069	16964	Attempted Murder	1	SF	03/04/21	03/10/21	05/14/21	
21010282	16962	Sex Offense	1	VSS	03/08/21	03/09/21	07/02/21	
			2	VSS	03/10/21	03/10/21	07/02/21	
21010400	17027	Sex Offense	1	NYN	03/24/21	03/30/21	05/13/21	
21011730	17028	Rape	1	NYN	03/24/21	03/30/21	05/14/21	
21012113	17063	Homicide	2	EK	03/23/21	07/06/21	07/27/21	
			3	EK	06/15/21	07/06/21	07/27/21	
21012315	17636	Attempted Murder	3	EK	03/23/21	07/06/21	07/27/21	
21012352	17001	Sex Offense	1	AL	03/22/21	03/23/21	05/13/21	
21012686	17133	Homicide	3	SF	04/02/21	04/12/21	07/07/21	
			4	SF	04/08/21	04/12/21	07/07/21	
21012826	17465	Assault	2	SF	03/26/21	05/25/21	07/16/21	
21012836	17044	Attempted Murder	2	CAG	03/25/21	07/23/21	09/23/21	
21012839	17211	Sex Offense	1	VSS	04/15/21	04/20/21	08/25/21	

Attachment A: OPD Forensic DNA 2021 Annual Report

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
21013292	17033	Attempted Murder	3	SF	05/27/21	07/22/21	11/01/21	
21013311	17132	Sex Offense	1	RJ	04/01/21	04/02/21	05/24/21	
			2	RJ	04/08/21	04/08/21	05/24/21	
21013351	17214	Homicide	4	SF	04/14/21	06/09/21	07/23/21	
			5	SF	04/22/21	06/09/21	07/23/21	
21013825	17427	Sex Offense	1	SF	05/12/21	05/19/21	07/28/21	
			2	SF	05/12/21	05/19/21	07/28/21	
21015947	17192	Homicide	1	AL	04/12/21	07/28/21	11/19/21	
21016024	17251	Sex Offense	1	CAG	04/14/21	04/26/21	06/11/21	
21016026	17315	Homicide	2	AL	04/29/21	05/04/21	07/09/21	
21016247	17196	Homicide	1	NYN	04/12/21	08/04/21	10/27/21	
21016388	17348	Rape	1	EK	05/04/21	05/13/21	06/15/21	
21016434	17351	Homicide	2	EK	05/06/21	05/10/21	05/25/21	
21016758	17260	Rape	1	CAG	04/22/21	04/27/21	06/25/21	
21016959	17261	Rape	1	CAG	04/21/21	04/27/21	06/18/21	
21017651	17317	Homicide	2	AL	04/23/21	05/04/21	06/04/21	
21017862	17269	Sex Offense	1	SF	04/21/21	04/28/21	07/19/21	
			2	SF	07/26/21	08/06/21	12/09/21	
21018029	17293	Rape	1	NYN	04/29/21	05/03/21	07/13/21	
21018445	17349	Burglary	1	EK	05/03/21	05/13/21	06/14/21	
			2	VSS	05/24/21	05/26/21	08/06/21	
21019226	17350	Rape	1	EK	05/06/21	05/13/21	06/15/21	
21019256	17430	Burglary	3	VSS	05/21/21	05/26/21	08/10/21	
21019404	17428	Rape	1	NYN	05/07/21	05/20/21	06/16/21	
21019875	17429	Rape	1	NYN	05/10/21	05/20/21	09/20/21	
21020232	17464	Sex Offense	1	SF	05/17/21	05/24/21	07/21/21	
21020353	17463	Rape	1	SF	05/12/21	05/24/21	07/27/21	
21020428	17481	Rape	1	VSS	05/26/21	05/26/21	09/03/21	
21020752	18291	Weapons	2	CAG	03/11/21	10/20/21	12/06/21	
21021725	17702		1	VSS	06/24/21	07/13/21	08/17/21	
21021747	17925	Rape	1	EK	08/06/21	08/16/21	10/14/21	
21022351	17472	Rape	1	SF	05/19/21	05/26/21	06/24/21	
21022361	17482	Rape	1	VSS	05/20/21	05/26/21	08/10/21	
			2	VSS	07/07/21	07/14/21	09/20/21	
21022554	17675	Sex Offense	1	EK	06/30/21	07/08/21	08/16/21	
21023021	17926	Homicide	1	EK	06/22/21	08/19/21	10/15/21	
21023596	17565	Rape	1	NYN	06/16/21	06/24/21	09/24/21	
21023657	17480	Sex Offense	1	VSS	05/25/21	06/10/21	07/21/21	
			4	VSS	05/26/21	05/26/21	07/21/21	

Attachment A: OPD Forensic DNA 2021 Annual Report

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
21023657	17480	Sex Offense	6	VSS	05/27/21	06/10/21	07/21/21	
21023776	17541	Homicide	1	AL	06/04/21	06/14/21	07/16/21	
			4	AL	08/09/21	08/11/21	10/27/21	
21023806	17556	Homicide	2	NYN	06/04/21	06/17/21	06/29/21	
21023847	17519	Rape	1	EK	05/28/21	06/08/21	09/13/21	
21024105	17696	Homicide	1	VSS	06/21/21	07/14/21	09/02/21	
			5	VSS	07/07/21	07/14/21	09/02/21	
21024541	17927	Rape	1	SF	08/12/21	08/16/21	11/19/21	
21024587	17703	Weapons	1	VSS	06/24/21	07/13/21	08/18/21	
21024838	17566	Sex Offense	1	NYN	06/17/21	06/25/21	07/26/21	
			2	NYN	06/17/21	08/06/21	10/13/21	
21025136	17602	Carjacking	2	SF	06/08/21	06/28/21	07/26/21	
			4	SF	06/24/21	06/28/21	06/29/21	
21025432	17611	Weapons	1	SF	06/04/21	06/29/21	09/22/21	
21025640	18016	Other Person	1	SF	06/10/21	08/27/21	12/03/21	
21025834	17557	Rape	1	NYN	06/10/21	06/24/21	09/20/21	
			3	NYN	07/13/21	07/15/21	09/20/21	
21026602	18025	Sex Offense	1	CAG	08/26/21	08/31/21	12/01/21	
21027249	17601	Sex Offense	1	SF	06/16/21	06/25/21	09/20/21	
21027433	17676	Rape	1	EK	06/30/21	07/08/21	08/16/21	
21027774	17853	Rape	1	SF	08/03/21	08/09/21	10/18/21	
21028801	17677	Sex Offense	1	SF	06/30/21	07/19/21	10/08/21	
21029048	17852	Rape	1	SF	08/03/21	08/09/21	10/14/21	
21029061	17750	Sex Offense	1	AL	07/06/21	07/26/21	10/04/21	
21029125	17721	Sex Offense	1	SF	07/06/21	07/19/21	11/01/21	
21029353	17715	Rape	1	VSS	07/01/21	07/16/21	09/29/21	
21029534	17855	Carjacking	2	SF	07/27/21	08/09/21	12/15/21	
21029908	17851	Kidnapping	3	AL	08/05/21	08/25/21	09/23/21	
21030018	17729	Rape	1	SF	07/06/21	07/23/21	10/06/21	
21030055	17741	Sex Offense	1	SF	07/14/21	07/22/21	09/23/21	
21030348	17850	Attempted Murder	1	SF	07/06/21	08/11/21	12/13/21	
21030428	17929	Rape	1	EK	08/05/21	08/17/21	12/27/21	
21032011	17704	Homicide	1	VSS	07/13/21	07/14/21	08/17/21	
21032314	17752	Rape	1	NYN	07/19/21	07/26/21	12/01/21	
21032706	17757	Rape	1	AL	07/15/21	07/28/21	09/03/21	
21032766	17809	Homicide	1	NYN	07/20/21	08/04/21	11/01/21	
			3	NYN	09/07/21	09/16/21	11/01/21	
21032767	17810	Homicide	2	NYN	07/20/21	08/06/21	10/08/21	
21033192	17836	Rape	1	NYN	07/26/21	08/05/21	10/05/21	

Attachment A: OPD Forensic DNA 2021 Annual Report

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
21033238	17854	Rape	1	EK	08/03/21	08/09/21	10/14/21	
21033732	17837	Rape	1	NYN	07/21/21	08/05/21	10/08/21	
21035260	18024	Assault	1	CAG	08/13/21	08/30/21	11/05/21	
21036286	17965	Homicide	1	VSS	08/11/21	08/25/21	12/15/21	
21036524	18034	Sex Offense	1	CAG	08/12/21	09/01/21	12/13/21	
			2	CAG	09/02/21	09/03/21	12/13/21	
21036648	18035	Sex Offense	1	CAG	08/12/21	09/01/21	12/01/21	
21036778	17994	Rape	1	VSS	08/13/21	08/24/21	10/13/21	
21036830	17997	Sex Offense	1	VSS	08/13/21	08/24/21	12/30/21	
			2	VSS	08/24/21	08/24/21	12/30/21	
21038078	18058	Rape	1	SF	08/26/21	09/03/21	12/13/21	
21038138	18072	Rape	1	EK	08/30/21	09/07/21	12/30/21	
21038518	17975	Homicide	2	HW	08/23/21	08/25/21	10/13/21	
21039365	18164	Sex Offense	1	NYN	08/26/21	09/22/21	12/23/21	
21039732	18064	Sex Offense	1	CAG	08/26/21	09/03/21	11/19/21	
21039816	18043	Officer Involved	2	CAG	08/31/21	09/20/21	12/22/21	
21039881	18074	Rape	1	AL	08/30/21	09/07/21	10/14/21	
21039973	18161	Rape	1	SF	09/08/21	09/21/21	12/06/21	
21040919	18192	Rape	1	SF	09/02/21	09/27/21	12/13/21	
21041052	18076	Homicide	3	AL	09/03/21	09/08/21	10/13/21	
21045076	18342	Homicide	1	HW	11/05/21	11/08/21	12/07/21	
21046897	18241	Rape	1	HW	10/08/21	10/08/21	10/29/21	
21049455	18292	Attempted Murder	2	CAG	10/22/21	10/22/21	12/09/21	
			6	SF	11/01/21	11/02/21	12/08/21	
			7	SF	11/01/21	11/02/21	12/08/21	
			8	SF	11/03/21	11/03/21	12/08/21	
			10	CAG	11/22/21	11/23/21	12/30/21	
21051405	18341	Assault	1	HW	11/05/21	11/08/21	12/17/21	
70054254	16965	Cold Case	2	VSS	02/29/12	04/21/21	09/29/21	
84007346	17057	Homicide	2	RJ	02/17/21	03/31/21	05/17/21	
90080996	17188	Rape	1	SF	09/25/20	04/15/21	06/29/21	
90111076	17453	Rape	1	SF	09/25/20	05/24/21	08/05/21	
91004254	17189	Rape	1	CAG	08/27/20	04/15/21	06/28/21	
91025384	17190	Rape	1	SF	08/27/20	04/15/21	06/29/21	
91032319	17191	Rape	1	AL	09/01/20	06/08/21	06/23/21	
91049814	17234	Rape	1	VSS	09/25/20	04/22/21	05/26/21	
91100433	17294	Rape	1	AL	09/29/20	05/03/21	06/02/21	
91116792	17233	Rape	1	VSS	09/29/20	04/22/21	05/24/21	
91133790	17295	Rape	1	AL	09/01/20	05/03/21	06/11/21	

Attachment A: OPD Forensic DNA 2021 Annual Report

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
91138313	17296	Rape	1	AL	09/01/20	05/03/21	06/03/21	
93115065	17341	Rape	1	EK	09/02/20	06/08/21	09/08/21	
94087483	16402	Homicide	1	HW	11/03/20	11/23/20	02/09/21	
95065901	17525	Rape	1	CAG	09/02/20	06/08/21	08/09/21	
97098610	17963	Rape	1	EK	09/03/20	08/19/21	10/15/21	
98079335	16501	Cold Case	1	SF	10/27/20	12/07/20	04/13/21	

430 requests for 218 new cases completed.

430 requests and 218 new cases completed.