CITY OF OAKLAND

Privacy Advisory Commission

September 7, 2023 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
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, **District 5 Representative**: Vacant, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, Vice Chair, **Mayoral Representative**: Jessica Leavitt*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. Call to Order, determination of quorum

2. Review and approval of the draft May 3 meeting minutes

3. Open Forum/Public Comment

4. Surveillance Technology Ordinance – DOT – Mobile Parking Payment System
    a. Review and take possible action on the proposed use policy

5. Surveillance Technology Ordinance – OPD – Fixed Wing Aircraft (with surveillance technology)
    a. Review and take possible action on a proposed use policy

CITY OF OAKLAND

Privacy Advisory Commission

May 4, 2023 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Regular Meeting Minutes

***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*

1. Call to Order, determination of quorum

In attendance: Chair Hofer, Gina Tomlinson, Lou Katz, Reem Suleiman, Chloe Brown, Gina Tomlinson, Robert Oliver, Jessica Leavitt

2. Open Forum

No public comment

3. PAC – Annual Election of Chair, Vice-Chair
    a. Nominate and elect officer
    Nominate Chair Hofer

    Chair Hofer asked members of the Commission if anyone wanted to run for the position of chair for one year. Commissioner Suleiman reminded Commissioners that a discussion during the retreat included figuring out a transition plan as several of the original board members terms start to phase out. An idea was proposed that Chair Hofer would continue as chair for one more year and put in place a transition plan to train the next Chair.

    Commissioner Suleiman made a motion that Chair Hofer continue as chair, which was uncontested. There was no opposition.

The motion passed unanimously

Chair Hofer requested nominations for Vice Chair. Chair Hofer nominated Commissioner Henry Gage as Vice Chair as his term will continue beyond many others on the Commission. Commissioner Gage was not present at the time of the nomination; however, the chair had earlier confirmed his interest to serve. Commissioner Brown seconded.

A voice vote was taken with seven Commissioners voting yes. There was one abstention by Commissioner Katz.

4. Surveillance Technology Ordinance – DPW – Illegal Dumping Cameras
    a. Third party sharing (Use Policy Sec. H) notice and report
    b. Review and take possible action, including to receive the report and possibly make recommendations to the City Council.

Chair Hofer introduced this item and indicated that under the Surveillance Technology Ordinance, there is a notice and report provision. Mr. Joe DeVries, the Chief Privacy Officer (CPO) provided a brief introduction of this issue during the retreat. The provision was activated by the Department of Public Works as it pertains to the illegal dumping camera program. As required by the ordinance staff proactively contacted the Chair of the Privacy Advisory Commission and the Chief Privacy Officer.

Victoria Chak, Administrative Services Manager, Oakland Public Works, Bureau of the Environment provided an update on an incident captured on the cameras. She presented updates from a memo that was included in the agenda packet entitled: PAC Info Memo OPD Video Data Request Data Sharing Final signed. The incident occurred near Wood Street as this area is a chronic dumping hotspot with repeat, opportunistic dumpers taking advantage of the blighted conditions in the area. The incident occurred on April 12, 2023 in the midst of operations to close the Wood Street encampment.

Ms. Chak reported that OPW received a request from the Oakland Police Department (OPD) to receive video data from one of the Wood Street pods. Staff complied with the 72-hour notification to the PAC chair and the CPO. As stipulated in the illegal dumping surveillance camera use policy details of the sequence of events are captured in the informational memo.

Chair Hofer stated that the larger concern in these issues is to compare the requirements of the use policy and the ordinance. The PAC needs to review the policy that's been approved and measure compliance. The City Council agreed that to avoid mission creep as the cameras would be limited to illegal dumping footage; refers back to OPD policy general

order J04. The crimes were not violent, however, violent forcible crimes could potentially be viewed if captured. OPD secured a warrant and due process was honored.

Joe DeVries indicated that staff would like to hear the Commissions thoughts on this matter. Staff did not contemplate potential litigation when crafting the ordinance and the request that we set aside a unit, which is technically a violation since the data is not being overwritten, but it's also not being shared at this time. The due diligence is being done in this case. This is an issue to consider for this technology and future technologies when there is potential litigation. Chair Hofer indicated that the policy does not state what happens pursuit to a court order or warrant not spelled out in the policy. It is stated in other policies established by the PAC.

Vice Chair Katz indicated that the ad hoc can consider the illegal dumping cameras along with the ALPR policy. The ad hoc could consider any potential litigation and how to handle in the instance of a court order. Staff is working with the City Attorney's Office to determine policy amendments. The proposed changes can be discussed by the ad hoc committee in advance of the item returning to the PAC.

Commissioner Katz made a motion to accept the report and Chair Hofer seconded the motion. The item passed unanimously.

5. Dept. of Transportation – Speed Safety System Pilot Program
    a. DOT will present on AB 645 and request a motion of support for the bill. The SOS Initiative aims to prevent severe and fatal traffic crashes, eliminate injury inequities, and carefully assess and mitigate any equity impacts resulting from safety measures. As part of its work, the SOS Initiative has supported the piloting of automated speed enforcement systems in Oakland to address the traffic violence on Oakland city streets and the disproportionate impact traffic violence has on Black, Indigenous, and People of Color communities, seniors, children, and people with disabilities.
    b. Review and take possible action

Tony Dang, Senior Advisor for policy and intergovernmental affairs for DOT made a presention on behalf of the Safe Oakland Streets Initiative which is an interdepartmental collaboration between the CAO, OPD, DOT, DVP and the department of race and equity. He was seeking support for AB 645 which authorizes a select number of cities in California to establish a pilot automated speed enforcement program. Currently, state law prevents any city from setting up a program. The bill would authorize 6 cities to set up a time limited five-year pilot program and require the cities to conduct and evaluation for effectiveness. Further action from the state would be needed to continue programs beyond 2032. A presentation and text of the legislation was included in the agenda packet. Mr. Dang provided highlights of the bill, including that only photographic evidence is allowed, no use of video.

Mr. DeVries clarified that a use policy and impact report would need to come back to the PAC.

Commissioner Officer Robert Oliver indicated that no operational motors unit in 2022. Research as shown that having an officer present does reduce speed for about one week, however; a camera reduces vehicle speed over a much longer period of time. OakDot will use an equity lens, schools and the high injury network when implementing the policy, if it passes at the state level.

Commissioner Gage inquired about a fee schedule; can you adopt one higher than in the legislation. Staff indicated that the fee schedule is prescriptive.

Commissioner Tomlinson is requesting more information about the locations. Staff indicated that it be provided after the use policy and community outreach efforts are completed. Lots of community members will be engaged in the process.

Commissioner Gage made a motion to accept the report, endorse the draft legislation and make a recommendation to council to do the same. Commissioner Suleman seconded the motion. The motion passed unanimously.

During the discussion, Chair Hofer highlighted that the Privacy Commission does not find significant privacy intrusion sufficient to oppose this bill. Commissioner Suleiman indicated that the purpose of the endorsement is to support the privacy aspects of the legislation.

Roll call:
D1 yes
D2 yes
D3 yes
D4 no
D5 absent
D6 abstain
D7 yes
Mayoral - yes
At-large – yes

The motion passed.

6. Surveillance Technology Ordinance – OPD – Annual Reports
    a. Review and take possible action on the annual reports for ShotSpotter, Cell-Site Simulator, Unmanned Aerial Vehicles/Drones, Live Stream Camera, and Mobile Fingerprinting ID

OPD moved to approve five annual reports that are required as part of the surveillance ordinance. Dr. Beckman clarified that the reports are for the year of 2022. He called attention to section G of the report

that refers to a statement from the information technology department about the ransomware attack. OPD's research indicates that there was no unauthorized access or breaches.

Chair Hofer moved to accept the Annual Report on the cell site simulator. Commissioner Brown seconded the motion.

Commissioner Katz asked did OPD have a cell cite stimulator and Dr. Beckman reported that they do not. The motion passed unanimously.

Chair Hofer proceeded to the Live Stream camera annual report.
Motion made by Chair Hofer, second by commissioner Katz. No one opposed or abstained.

The next annual report discussed was Mobile ID. Chair Hofer had a question regarding the system that former Sherriff Ahern received a $600k biometric system and there was a large number of storage purchased and significant upgrades. Chair Hofer indicated that if the system was getting larger then the policy might need to be revisited.

Officer Pullen indicated that OPD returned all their equipment to the Sherriff's department and have not gotten it back since the upgrade occurred. He indicated that it was returned for software upgrades. He indicated that they planned to engage again in the future.

Chair Hofer moved to accept the item. There was a second by Commissioner Brown. There was a voice vote with no opposition or abstentions.

The next OPD report discussed was the drones. Chair Hofer stated that he believed the report possibly needed to be re-written. The issue that needs to be resolved is to track the use of the technology. It's difficult to determine the benefits of the technology. In section H, for example there is a table of Oakland crime data and with that information alone it is difficult to determine causation. In this case with flight logs and other auditing and tracking that should occur where the volume isn't large like body worn cameras and license plate readers it would be helpful to determine the link between the usage of drones and solving crimes. The annual report does not mention anything about the drones' solving crimes.

Lt. Febel, Special Operations Section provided an update on the drones annual report. He explained that this will now be governed by military equipment annual report and there are very stringent requirements under AB 481 and the departments I25 policy and the local municipal code. The Police Commission and City Council approved policies to oversee the technology. The tracking of all military equipment, drones are subject to that same reporting and tracking. There is a system being developed through a comprehensive Vision database to track a variety of data points, including where the drones are being deployed, any related complaints and who is affected by the technology. The 2022 data is going to presented to the Police Commission for AB 481 for the period July 2022 to January 2023.

Commissioner Gage emphasized the need for data to make informed decisions and advocate for resources. Commissioner Oliver requested a copy of I25.

Hofer recommended tabling the drones item until the data is presented to the PAC and requested that the item come back in June.

The final annual report discussed was ShotSpotter. Commissioners asked questions regarding the cost per year for ShotSpotter which was covered in the report. Lt. Steve Valle responded and indicated that a response to the question was covered in the report and the cost was $798,486.00.

Commissioners raised a range of questions regarding ShotSpotter and third-party data sharing. Lt. Valle, indicated that ATF does not have access to the system. It did state in the annual report that ATF has access, this is incorrect and needs to be corrected. Chair Hofer stated that 3rd party data sharing section needed to be revised in the annual report to reflect that the Oakland Housing Authority (OHA) does have access to the system and they are authorized users. Lt. Valle explained that OHA has properties all over the city and many are in high crime areas where gun fire takes place and providing OHA access to shots potter is a benefit to respond to crime scenes quickly. OHA's access to ShotSpotter information is not in the approved use policy. The 3rd party data sharing agreements may need to be changed to reflect the current or needed uses of the technology.

Chair Hofer requested that the ShotSpotter annual report return to the PAC to address the PAC's 3rd party data concerns.

7. Surveillance Technology Ordinance – DOT – Parking Mobile Payment System
    a. Review and take possible action

Chair Hofer introduced the item and requested information about the provider. He indicated that this could be sent to an ad-hoc. The PAC was waiting on the contract to make sure everything matches with the proposed use policy. It's also important to consider the adopted privacy principles in the process.

Michael Ford with the Department of Transportation stated that the current extension goes through August. The most important aspect of the contract is the scope of work (attachment A). Mr. Ford indicated that he welcomes the opportunity to sit down with the ad-hoc.

Chair Hofer raised a question about when the law clinic students were meeting with Mr. Ford and DOT staff it was clear that a data map is developed. It's important to figure out the verification process. There is a need to verify and protect personally identifiable information (PII) data.

Commissioner Oliver had a number of questions about the parking system and how citations are issued. Citations are issued once a day if the vehicle is left in the same location. Once a valid citation is written then the registered owner will be held accountable for it and the citation is mailed to them.

Chair Hofer requested to know if the vendors had a privacy policy under SB 34 which is the state law that pertains to license plate readers. SB 34 governs privacy issues for some companies and their complaint polices are stated on websites.

An ad hoc will be convened to work with Mr. Ford on the vendor contract, use policy and/or impact statement.

The meeting was adjourned.

ANTICIPATED IMPACT REPORT - REVISED DRAFT
Mobile Parking Payment Systems for
Parking Management and Enforcement

Michael P. Ford
Parking & Mobility Division
Department of Transportation
City of Oakland
August 23, 2023

0. Definitions

Parking data
Any logbooks, records or data files used or created pursuant to a parking payment service including electronic storage media, Software, Source Code, any database and database rights, personal or personally identifiable information relating to an identified or identifiable individual, payment transaction, parking session or data transmission, including the originating and destination numbers and internet protocol address, date, time and duration, information on a vehicle, customer, location or payment media. This data may contain personally identifiable information (PII).

Personally identifiable information
Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Raw Parking Payment Transaction Data
A subset of Parking Data that includes parking date, start and end times for each transaction, payment amounts, transaction fees for the Providers, numbered “zones” corresponding to parking location and customer data including license plate number, customer ID or other information about the customer and their payment media. This data may contain PII.

Unprocessed Anonymized Data
A subset of Raw Parking Payment Transaction Data that only includes parking transaction date with start and stop times for each transaction, meter payment amounts, user transaction fees for the Providers, and numbered “zones” corresponding to parking location. This data does not contain any PII or data on the customer except for the vehicle’s license plate number.

Aggregated Anonymized Data
A summary of Unprocessed Anonymized Data that Contains ONLY a sum of the total number of parking payment transactions that occurred on each block face during each one-hour period of each day and the total revenue received from the sum of those transactions. In any case where three or fewer transactions occurred on any given block face during any given hour, such data will be obfuscated to a default number. This will allow staff to know that a small amount of

transactions occurred and revenue was collected, but also ensure that there is no record of any individual transactions. Therefore, this data does not contain any individual transaction data or customer data. This data does not contain any PII and cannot be used to re-identify anyone or their location.

Provider
A business whose services allow individuals to pay for parking sessions through a mobile phone application (app), website, or text message in Oakland and which has all necessary licenses and registrations to conduct such business.

Third Party Data Contractor
Any business contracted by the Provider to provide any service that may include accessing, storing or viewing Parking Data generated in Oakland.

System Security Plan
A plan submitted by each Provider detailing the data security, storage, and encryption practices that meet or exceed industry standards, including Payment Card Industry Data Security Standard (PCI-DSS) and System and Organization Controls 2 [e.g., (SOC 2). DOT expects that these best practices will primarily address user payment methods to protect credit card information. The Plan must also address how the Provider plans to prevent and respond to cyberattacks, including:

- Process for keeping software up to date;
- Monitoring systems and networks for malicious activity;
- Use of secure uniform resource locators (URLs)
- Employee education and training;
- Who is responsible for reporting the attack to the appropriate authorities;
- How customers and others will be alerted;
- How Provider will discover what data and what kind of data was stolen;
- How the Provider will comply with CA Senate Bill 34; and
- Changing and strengthening passwords.

1. Information Describing the Proposed Data Sharing Agreement and How It Works

The City of Oakland (City) Department of Transportation (DOT) intends to enter into agreements with each of the six selected providers (Providers), including:

- PayByPhone US Inc. (PayByPhone),
- Passport, Inc. (Passport),
- ParkMobile, LLC (ParkMobile),
- HonkMobile USA Ltd. (Honk),
- Marina Security Services, Inc. and Mortimer Smythe LLC (Oakland Parking Solutions), and
- IPS Group, Inc. (IPS).

These Providers' services permit individuals to pay for parking sessions through their mobile phones in Oakland. With these services, parkers will be able to initiate a parking session through a mobile phone application (app), website, text message, or phone call, depending on the Providers' services. To initiate a parking session, parkers are required to enter their payment information (such as a credit card or Google Pay), "zones" corresponding to City blocks, and license plate number on the Providers' app. Oakland is implementing "demand-responsive" parking areas in which parking fees may vary from block to block in order to reflect demand. So far, this has been limited to the Montclair business District and Chinatown, but will be expanded to all commercial areas. Each block in metered areas has a unique "zone" number. In demand-responsive areas, zones will correspond to a City-provided Facility ID printed on new parking signs and will not differ by Provider. In all other metered parking areas prior to demand-responsive rates being implemented, the Provider-created ID per block will be used. When choosing to pay by app, customers must enter the zone number within the Provider's platform. Zones are shown in Providers' apps and on signs.

DOT uses Unprocessed Anonymized Data from mobile parking payment Providers in order to enforce parking restrictions, such as time limits and meter payments, to analyze parking revenues and demand, and to review citation disputes. License plate and zone information are pushed to DOT's Automated License Plate Readers (ALPR)[1] through an application programming interface (API) between other vendors who support the City's parking enforcement system. Parking Control Technicians use ALPR to scan vehicles' license plates and check for an active paid parking session associated with the license plate and location (numbered zone).

In addition to pushing data to enforcement technologies, the Providers also collect data from parking sessions and "publishes" these datasets to an online platform that authorized staff can access through a unique username and password. The Unprocessed Anonymized Data published to the online platform will include license plate number, parking date and start and stop times, payment amounts, transaction fees for the Providers, and "zones" corresponding to parking location. This data will include no personally identifiable information, and DOT staff will use this data for financial and parking analyses and for responding to parking citation disputes. All Unprocessed Anonymized Data will be deleted after one year. DOT staff will also have access to, or may create, Aggregated Anonymized Data to analyze and summarize historical parking data by block face, date, hour and revenue collected. Aggregated Anonymized Data may be retained indefinitely.

In receiving Unprocessed Anonymized Data, DOT can ensure that programmed parking rates and time limits are accurate and parking citations are correctly issued. For example, in an event a parker disputes a citation due to having a paid ParkMobile session, the parking payment can be properly reconciled, particularly in demand-responsive parking program areas.[2] In these

[1] See the Privacy Advisory Commission's approved use policy and anticipated impact report for automated license plate readers. Available online at: https://www.oaklandca.gov/documents/automated-license-plate-reader

[2] More information on ParkOakland, the Demand-Responsive Parking & Mobility Management Initiative, is available on the City's website here: https://www.oaklandca.gov/topics/park-oakland

areas, meter rates change by time of day and Value or Premium Rate area. DOT will ensure that zones would be visible in the transaction data in order to program these specific areas' rates or audit the accuracy of Providers' rates/revenues. The importance of this auditability recently came up regarding the demand-responsive rates at the La Salle Garage and in Montclair, where time-of-day pricing was not correctly programmed in ParkMobile's app and showed this incorrect pricing to parkers. This error had financial implications but was able to be corrected through the portal and through ParkMobile's client support services.

The professional service agreements with each Provider will allow Providers to share Unprocessed Anonymized Data, including location-based information corresponding to numbered block zones, with DOT. Importantly, the agreements will require that certain data is excluded from the portal in order to better protect individual parkers' privacy (see excerpt below). DOT staff will be able to access up to one (1) year of Unprocessed Anonymized Data in each Provider's online portal. If a contract between a Provider and the City is severed, then the Provider will be required to delete all Raw Parking Payment Transaction Data collected in Oakland. City staff will not have access to Raw Parking Payment Transaction Data in this portal. For additional details, see the draft "City Data Addendum" to the City's Professional Services agreement (Attachment A).

The contract term is for up to seven years, including two optional years, and in an annual amount not to exceed $900,000 in Providers' transaction fees collected from parkers in Oakland.

DOT staff have aimed to procure the most secure mobile parking payment system through the RFP process. The Request For Proposals (RFP) was issued in March 2022, and proposals were due in April 2022. DOT staff received seven proposals, of which six were deemed Responsive. When DOT staff initially presented the next-generation mobile parking payment system to the PAC in April 2021, data security for users was a key component of discussion. The Commission's comments were adopted into the RFP, primarily through the following scope section:

> ***1.4 Data Privacy Requirements.*** *One of the key goals of this new pay-by-phone system is to enhance user data protections. The system must comply with the City's Surveillance Technology Ordinance (Oakland Municipal Code Chapter 9.64) and subsequent system use policy and anticipated impact report in the following capacities:*
>
> - *Maintain an online system portal/back-office system with **none** of the following information visible to staff at any time for any reason:*
>   - *Personally identifiable information (PII), including but not limited to, name, phone number, home address, email address and credit card information*
>   - *Individual user account details*
> - *Provide a System Security Plan with data security, storage, and encryption practices that meet or exceed industry standards, including Payment Card Industry Data Security Standard (PCI-DSS) and System and Organization Controls 2 [e.g., (SOC 2). DOT*

expects that these best practices will primarily address user payment methods to protect credit card information.

- *Disclose any additional companies who would support or follow the Provider's System Security Plan, such as third-party cloud storage services.*
- *Ensure the security of user and transaction data through System Security Plan protocols per current industry standards of PCI-DSS and SOC 2.*
- *Provider must comply with the City's Surveillance and Community Safety Ordinance (Oakland Municipal Code Chapter 9.64), the approved use policy regarding the mobile parking payment system, and any other relevant surveillance laws relevant to Oakland, California.*

Notably, parkers are not required to use the mobile parking payment system in on- or off-street facilities in Oakland. The California Vehicle Code requires that parking meters must be operable in order to write a defensible citation; in other words, parking payment for a space cannot only be accepted by nonphysical means like an app or website (CVC Section 22508.5(d)).[3] While there is no anticipated possibility that parkers will be required to use the new mobile parking payment system in Oakland, DOT staff seek to implement a system that meets, if not exceeds, the requirements of the Surveillance Technology Ordinance.

DOT staff worked with Contract Services and the City Attorney's Office to include the requirement to comply with the approved use policy and impact report for this system in the Professional Services Agreement. By including this requirement as an addendum of the standard professional services agreement (see Attachment A), the City will have greater capability to enforce this requirement in the event of non-compliance. The agreement as edited by the City Attorney's Office can be found in **Appendix D**.

2. Proposed Purpose

Data from mobile parking payment services may help shape parking policies, plans, and practices in Oakland. Analyses of this data guide staff's active management of the parking system and access to finite, valuable curb space. Importantly, this data is also used in the issuance of citations and the review of citation disputes. Mobile parking payment services expand the available payment options for parkers, in turn increasing the convenience and ease of parking. Making parking easy and more actively managing the parking system are two of the City's Parking Principles (Resolution No. 84664 CMS) and shape a more equitable mobility system.

Under the current mobile parking payment system, a single Provider is permitted to operate in Oakland. From 2015 to 2019, parking payments made through this Provider comprised about 10% to 15% of the City's total on-street parking revenue, generating a total of approximately $6.5 million in parking revenues. Signage promoting this Provider's brand is currently posted in the public right-of-way (PROW) but given maintenance challenges, is not always readable. The

[3] This CVC section is available online here: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=VEH&sectionNum=22508.5

City's current Provider, ParkMobile, also supports ongoing pilots at the LaSalle Garage in the Montclair District and the Telegraph Plaza Garage to integrate the City's off-street facilities into the on-street system and thus, eliminate costly one-time expenses such as traditional parking access and revenue control systems (PARCS), and ongoing expenses, such as administrative and accounting overhead, maintenance of equipment, and back-office labor. This integration was adopted by City Council in the Fiscal Year 2021-2022 Budget.

DOT has pursued an enhanced multi-vendor mobile parking payment system for several reasons: 1) increase the convenience of this service to parkers, 2) promote the use of this contactless payment method with City-branded signs in the PROW, and 3) more holistically support the active management of the parking system. A key improvement will be City of Oakland-branded signs that will direct parkers to a webpage with all available Providers and promotions, as well as supporting future pilots and innovations like the LaSalle Garage. Existing ParkMobile signs that display the zone number are currently in a state of severe disrepair, when they are still present on-street at all (see **Figure 1**). New City-branded signs will be printed and installed in demand-responsive project areas in phases, as meter rates are adjusted and Value and Premium Rate areas implemented (see **Figure 2**). Signs in Montclair and bilingual signs in Chinatown have been implemented first. Providers will contribute to the costs of installing and maintaining the system, particularly signs, through a one-time up-front fee of $190,000 (split across all selected Providers) and 10% of ongoing user fees. In addition to these fees, Providers may run their own marketing campaigns aimed at parkers in Oakland.

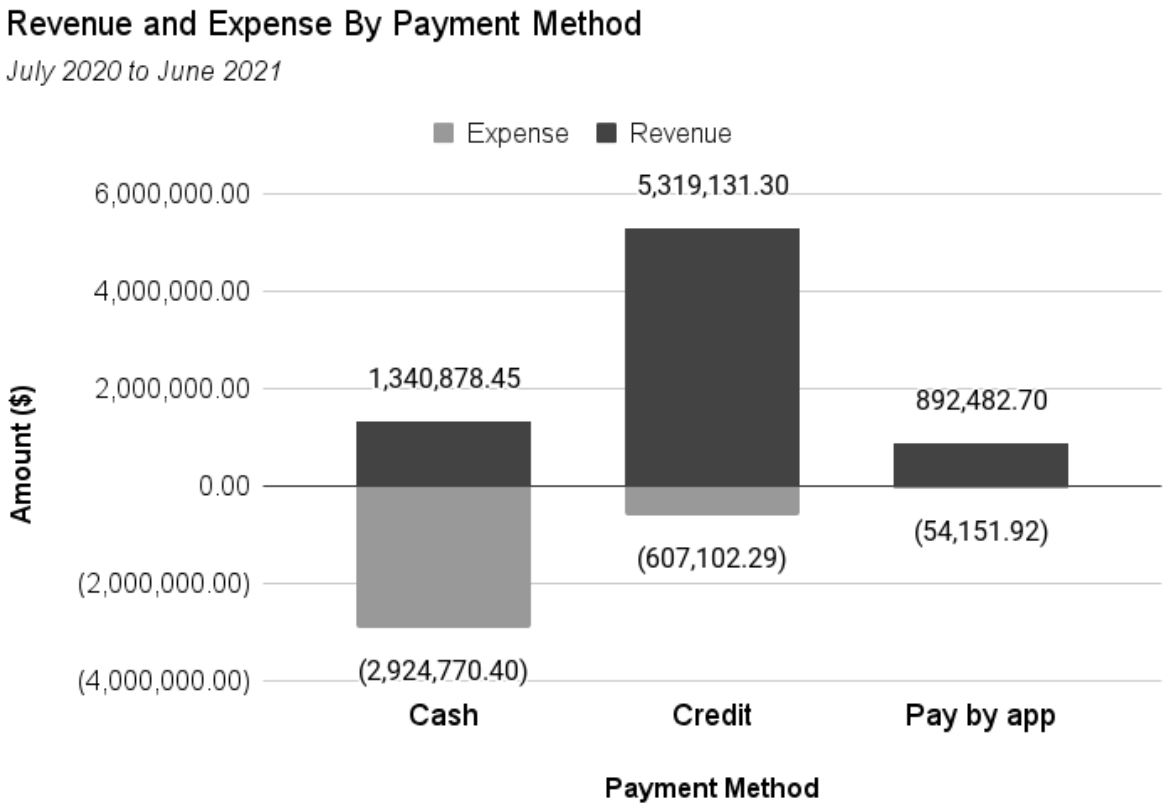
Figure 1: Existing Pay Here + Mobile Parking Payment Signs

Figure 2: New Approved Pay Here + Mobile Parking Payment Signs

The mobile parking payment system provides several key advantages to both parkers and the City that contribute to the importance of this system. The mobile parking payment system meets rising demand for contactless payment options and supports the health and safety of consumers by reducing touch-points.[4] It is anticipated that positive consumer experiences with contactless payments, including the City's pay-by-app parking services, will make more individuals interested in using this payment type, even as the pandemic continues to subside. Additionally, the City pays lower fees for parking transactions made by app than transactions made by coin or credit/debit card (see **Figure 3**). In Fiscal Year 2020-2021, 6% of parking revenues paid by app were spent on fees and expenses, compared to 11% spent on credit/debit card expenses and 218% on coin expenses.

Figure 3: Revenue and Expense by Payment Method (July 2020 to June 2021)

[4] Retail Leader. "Will Consumers Stick With Contactless Payments?" August 6, 2020. Available online here: https://retailleader.com/will-consumers-stick-contactless-payments



By accepting multiple vendors to operate in Oakland, visitors will likely not need to download any additional applications (apps) and share their information with another Provider. Rather, they are more likely to be able to use an existing app on their phone and conveniently pay for their parking session. With this variety of Provider options available to parkers, the enhanced system is intended to minimize the number of Providers with whom users, especially visitors to Oakland, must share their information to pay for parking by app and maximize parkers' choices as consumers.

Residents will also benefit from having multiple vendor options, as vendors will compete for long-term customers with lower user fees and promotions, and from new community engagement requirements that aim to make Providers' services more equitable and inclusive. Each Provider's user fee and website will be clearly shown on the City's go-to parking resource webpage (oaklandca.gov/oakparkplus). A QR code and the URL to this webpage are shown on the new City-branded signs to be installed in demand-responsive project areas.

Specific applications of mobile parking payment data that supports this effort will include only the following:

a) Estimating parking demand, occupancy, and revenues
b) Evaluating parking payment options

c) Monitoring demand-responsive parking areas and compliance
d) Reconciling payment transactions with total parking revenues received
e) Promoting compliance and enforcing parking restrictions, permits, and payment
f) Reviewing contested parking citations
g) Remitting user transaction fees to Providers via invoices

3. Locations of Deployment

The data shared under this proposed agreement is user-generated within the City's parking system and therefore collected in all neighborhoods with parking meters or public parking facilities. Parking meters and public parking facilities are primarily found in commercial zones, near public transit stations, and in other areas with high demand for parking. Existing meters and Council-approved meter zones (OMC Section 10.36.140) are shown in this map: https://oakgis.maps.arcgis.com/apps/mapviewer/index.html?webmap=8fa241d70ab5494f8e50e678065d627b

Providers may begin operating in phases, such as if beta testing is required, and may start in certain geographic areas before operating at citywide scale. In this case, the geographic areas where Providers operate would be listed on the City's parking webpage to minimize any confusion to parkers and appropriately communicate how to use the mobile parking payment system.

4. Potential Impact on Civil Liberties & Privacy

DOT acknowledges the private and sensitive nature of personally identifiable information (PII) and block-level location data included in mobile parking payment data. Without mitigations, mobile parking payment data would be vulnerable to privacy risks such as re-identification, as users' names and contact information are typically collected by Providers and made available to their clients via the portal. In order to minimize, if not eliminate, privacy and surveillance risk, DOT has developed a set of guidelines based on feedback from the Privacy Advisory Commission received in March and April 2021 for how mobile parking payment data will be handled, aggregated and obfuscated to protect users' data, using mitigations outlined below. These mitigations were provided to prospective bidders in the recent competitive process for the enhanced mobile parking payment system; through their proposals, all six Providers have initially agreed to follow the mitigations below and this impact report and use policy, upon finalization and approval.

5. Mitigations

DOT recognizes the sensitive nature of parking and user data generated through mobile parking payment Providers and has developed the following guidelines for the responsible handling of this data:

1. Per the draft agreement scope (see **Appendix A**), DOT will not have access to any PII of parkers who use the Providers' services. The public may access anonymized minimally-processed data available in the portal through public records requests, subpoenas, warrants, and other court orders. This data will not be raw, as Providers will have removed PII and individual user account details from the portal.
    a. In the competitive process to procure the new mobile parking payment system, DOT issued the requirement below. All six proposed Providers have initially agreed to this requirement in their respective proposals. This mitigation would effectively eliminate privacy risk by anonymizing parking data.

    - *"Maintain an online system portal/back-office system with **none** of the following information visible to staff at any time for any reason:*
        - *Personally identifiable information (PII), including but not limited to, name, phone number, home address, email address and credit card information*
        - *Individual user account details"*

2. DOT has sought and selected Providers whose data security, storage, and encryption practices follow a System Security Plan. All Providers currently and must continue to maintain Payment Card Industry Data Security Standard (PCI-DSS) and System and Organization Controls 2 (SOC 2) compliance. Additional privacy and security measures, such as California Consumer Protection Act compliance, differ between Providers but are available in their respective privacy policies (see **Appendix B**).
3. After each agreement has been signed and executed, login credentials to the Providers' online portals will be unique to each authorized staff who has been granted access to the mobile parking payment data. Login credentials will not be shared outside of authorized staff in DOT and Finance.

6. Data Types and Sources

In this proposed system, the Providers will "publish" Unprocessed Anonymized Data on their respective online portals that are only available to City staff. While these platforms vary by Provider, parking data available within the platform will include the following:

- Numbered zone indicating approximate parking location
- Parking date and start and end times
- Parking transaction amount
- Transaction fee (to be paid to the Provider)

Provider's portals primarily differ by aggregate data analyses, such as charts and graphs showing growth over time in Oakland parking transactions made by app. Importantly, as stated in the previous section no Provider will show PII or individual user account information in the portal at any time for any reason.

License plate number data is necessary for both enforcement purposes and for responding to parkers' citation disputes. License plates are scanned or entered by Parking Control Technicians in automated license plate readers (ALPR) to check if the vehicle has an active parking session. All citations issued require that a license plate number be inputted, and the handheld device prohibits a Parking Control Technician from issuing and printing the citation if there is an active ParkMobile session associated with the plate. In the event that a parking citation is disputed, then this request is processed and analyzed by the Parking Citation Assistance Center Staff. Currently, staff look up the license plate number in ParkMobile's portal and verify their parking session by license plate, zone number, and parking session date and start time. Without being able to view license plate information, Parking Citation Assistance Center staff would have to rely on vendors to look up this data, which would pose a significant burden on the Center's processing time and resources.

Only authorized staff in DOT and the Finance Department with unique usernames and passwords may log in and access this data, unless requested through a public records request.

7. Data Security

Each provider responded with details regarding their own unique data security protocols. Per the draft agreement section in Section 1 of this impact report, DOT is requiring that each Provider securely store, publish, and audit the data according to industry standards and best practices outlined in their System Security Plan. Providers are required to provide a fully auditable mobile parking payment service. DOT or Finance staff will audit Providers through their respective back-end online data portals, in addition to Providers going through PCI DSS audits. Audits by DOT or Finance staff will occur on an as-needed basis, such as audits of a subset of zones where meter rates were recently changed.

Upon execution of the draft Professional Services Agreements (see **Appendix A**), Providers are required to provide a current certification through the Payment Card Industry Data Security Standards (PCI DSS). All Providers currently meet these standards. Major Providers such as ParkMobile, Passport, and PayByPhone maintain PCI DSS Level 1 certification. Smaller Providers may maintain a lower level due to the smaller number of annual transactions processed through them. PCI DSS certification was the primary security requirement that the City sought when procuring mobile parking payment services in 2015 and continues to be industry standard. Procurement of the new mobile parking payment system has sought to maintain and exceed this standard through additional privacy and security requirements by disclosing data storage and encryption practices and PII protection.

Auditability was also a requirement of the 2016 agreement between the City of Oakland and ParkMobile, and ParkMobile has published information regarding account and payment security on its website: https://support.parkmobile.io/hc/en-us/articles/203299650-Is-my-account-and-credit-card-information-safe-.

More information on individual users' data security is available in five of the six Providers' existing user terms and conditions and privacy policies (see **Appendix B** and **Appendix C**). These documents are not yet available for Oakland Parking Solutions due to their app being a custom-build. However, all Providers will be required to comply with the terms included in the "City Data Addendum" (see **Appendix A**).

Regarding data retention, staff will require that Providers store only one (1) year of Unprocessed Anonymized Data in their respective portals in order to provide sufficient time for parking citation appeal processes. Providers will store Raw Parking Payment Transaction Data parking payment transaction data collected in Oakland for no more than one (1) year. If the contract between a Provider and DOT is severed, the Provider will be required per the signed Professional Services Agreement to delete all Raw Parking Payment Transaction Data
collected in Oakland (see **Appendix A**). If such an event occurs, the Provider will be asked to email the DOT Project Manager a confirmation that all raw data collected in Oakland has been deleted.

8. Fiscal Cost

Providers operate at no direct cost to the City of Oakland. Instead, parkers who use the Providers' services pay a fixed fee to the Provider per parking session, in addition to the cost generated by the meter. Currently, parkers pay $0.25 per transaction *plus* the amount of time that they wish to park according to the meter rates.[5]

To adhere to generally accepted accounting principles (GAAP), the draft agreement requires that the City collect all revenues for all parties, including the Providers' user fees. As a result, Providers will invoice the City monthly to receive their user transaction fees. This practice is consistent with the existing agreement and practice with ParkMobile.

Staff are anticipating an increase in parkers using mobile parking payment services under the enhanced system and have thus allocated up to $900,000 of user fees per year in the contract amount that will be reimbursed to the Providers. The Providers will only receive the reimbursed user transaction fees and will <u>not</u> receive any payment from the City. DOT staff have estimated a total of 14,000,000 transactions generated over the total contractual period across all Providers, including in the optional extension years. The contract amount has been set based off the maximum projected transactions per year (see **Table 1**).

Table 1: Estimated Parking Revenues and Transactions

	2019 Actual	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6 optional	Year 7 optional

[5] The Master Fee Schedule permits that meter rates may be adjusted between $0.50 and $4 per hour.

Total Estimated Parking Revenue	$14.6 million	$15.3 million	$16.1 million	$16.9 million	$17.8 million	$18.6 million	$19.6 million	$20.5 million
Estimated Parking Payment by Phone/App	13.40%	16.75%	20.00%	25.00%	30.00%	35.00%	40.00%	45.00%
Estimated Average Transaction Amount	$2.57	$2.60	$2.65	$2.70	$2.75	$2.80	$2.85	$2.90
Total Estimated Transactions	761,443	987,606	1,214,830	1,564,938	1,935,970	2,329,214	2,746,021	3,187,810

Additionally, selected Providers will contribute to the City's expenses to operate and maintain the enhanced mobile parking payment system, including but not limited to installing signs and reconciling the system's funds. At the beginning of the contract term, each Provider will pay their designated portion of the one-time upfront "start-up" fee of $190,000. Each Provider will also share 10% of their user fee revenues generated in Oakland with the City on an ongoing basis.

Currently, the user fee is $0.25 per transaction with ParkMobile. The proposed user transaction fees for each selected Provider are below (see **Table 2**). In the enhanced mobile parking payment system, user fees are expected to be a primary point of competition between Providers for parkers' business and loyalty. Providers may also compete through their marketing efforts, such as first-time user promotional codes. Per the draft agreement, the City may choose to waive user fees at any time and instead pay them on behalf of the parker.

Table 2: Selected Proposers' User Transaction Fees

Provider	User Fee (per user transaction)
PayByPhone	$0.25
Passport	$0.20 *Note: may include gateway fee (+$0.05)
ParkMobile	$0.40
Honk	$0.25
Oakland Parking Solutions	$0.30
IPS	$0.25

9. Third Party Dependence

Raw Parking Payment Transaction Data will be received and stored by the Providers on an ongoing basis and for up to one year. The City does not collect this data, nor does it have the means to store this data in compliance with industry standards. Most Providers, including the six selected Providers, rely on Third Party Data Contractors to securely store data. These detailed processes and services were provided in confidence in each Provider's proposal. However, third party authorization and use is broadly covered in the Use Policy and Data Addendum (see **Appendix B**). Because Oakland Parking Solutions is custom-building an app in order to operate in Oakland's mobile parking payment system, their privacy policy is not yet available for review.

10. Alternatives

The primary alternative to the proposed data sharing agreement is not enforcing any of the additional privacy or security features provided in the RFP. This may have reduced barriers to entry for Providers to Oakland's mobile parking payment system but would have resulted in a less secure mobile parking payment system. Because DOT staff received proposals from a range of Providers (large and small, local and not local) in the competitive process, this alternative may not have actually resulted in an "easier" proposal process for potential or existing Providers but certainly would have compromised the security of users' data in Oakland.

11. Track Record

Mobile parking payment services are available in cities throughout California, the United States, and the world. However, the City's 10 years of experience with mobile parking payment services is most pertinent to the purpose of this report. ParkMobile has been the City's Provider since 2011. In a typical year since 2015, about 10 to 15% (typically $1.5 to $2 million) of annual on-street parking payment transactions are made through ParkMobile. In addition to procuring a system with enhanced privacy and security measures, a key challenge with this service has been the maintenance of signage showing the zone number. Thus, a renewed investment in signage, including the initial start-up fee and ongoing revenue share, was a key component of the new system's RFP and innovative for the nature of this procurement.

In March 2021, ParkMobile experienced a data breach of over 20 million users' information. In an email sent by ParkMobile on April 13, 2021, DOT staff were notified of the following: "[Parkmobile's] investigation has confirmed that basic account information – license plate numbers and, if provided by the user, email addresses and/or phone numbers, and vehicle nicknames – was accessed. In a small percentage of cases, mailing addresses were affected. No credit cards or parking transaction history were accessed, and [Parkmobile does] not collect Social Security numbers, driver's license numbers, or dates of birth." In response to community members' concerns regarding the breach, DOT provided more information and resources about the breach on the City's website.[6] Staff did not discover any other reported data breaches from the other five Providers in their research.

Staff will not ask ParkMobile to migrate user information or data to the additional new Providers operating under the enhanced mobile parking payment system in order to avoid any compromise of the company's marketing and customer retention efforts. Rather, ParkMobile will now be competing with five (5) other Providers for parkers' business in Oakland. Providers will primarily compete through transaction fees and promotions but may also compete through their privacy policies and practices that enhance parkers' privacy.

The enhanced mobile parking payment system service supports the City's Parking Principles (Resolution No. 84664 CMS) by making parking easier and will be used as a pillar of the parking system. As cities increasingly move to multi-vendor mobile parking payment systems, the City continues to be on the forefront of innovation and data privacy standards through this next-generation mobile parking payment system. DOT staff are thrilled to be delivering a more secure system to parkers in Oakland that complies with the Surveillance Technology Ordinance and enacts the necessary mitigations to protect individual user data.

Questions or comments concerning this draft Impact Report should be directed to Michael Ford, Division Manager, Parking and Mobility Division, via email at mford@oaklandca.gov or phone at (510) 238-7670.

[6] This response is available here: https://www.oaklandca.gov/topics/parkmobile-march-2021-data-breach

USE POLICY - REVISED DRAFT
Mobile Parking Payment Systems for
Parking Management and Enforcement

Michael P. Ford
Parking & Mobility Division
Department of Transportation
City of Oakland
August 23, 2023

0. Definitions

Parking data
Any logbooks, records or data files used or created pursuant to a parking payment service including electronic storage media, Software, Source Code, any database and database rights, personal or personally identifiable information relating to an identified or identifiable individual, payment transaction, parking session or data transmission, including the originating and destination numbers and internet protocol address, date, time and duration, information on a vehicle, customer, location or payment media. This data may contain personally identifiable information (PII).

Personally identifiable information
Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Raw Parking Payment Transaction Data
A subset of Parking Data that includes parking date, start and end times for each transaction, payment amounts, transaction fees for the Providers, numbered “zones” corresponding to parking location and customer data including license plate number, customer ID or other information about the customer and their payment media. This data may contain PII.

Unprocessed Anonymized Data
A subset of Raw Parking Payment Transaction Data that Includes parking transaction date with start and stop times for each transaction, meter payment amounts, user transaction fees for the Providers, and numbered “zones” corresponding to parking location. This data does not contain any PII or data on the customer except for the vehicle’s license plate number.

Aggregated Anonymized Data
A summary of Unprocessed Anonymized Data that Contains ONLY a sum of the total number of parking payment transactions that occurred on each block face during each one-hour period of each day and the total revenue received from the sum of those transactions. In any case where three or fewer transactions occurred on any given block face during any given hour, such data will be obfuscated to a default number. This will allow staff to know that a small amount of

transactions occurred and revenue was collected, but also ensure that there is no record of any individual transactions. Therefore, this data does not contain any individual transaction data or customer data. This data does not contain any PII and cannot be used to re-identify anyone or their location.

Provider
A business whose services allow individuals to pay for parking sessions through a mobile phone application (app), website, or text message in Oakland and which has all necessary licenses and registrations to conduct such business.

Third Party Data Contractor
Any business contracted by the Provider to provide any service that may include accessing, storing or viewing Parking Data generated in Oakland.

System Security Plan
A plan submitted by each Provider detailing the data security, storage, and encryption practices that meet or exceed industry standards, including Payment Card Industry Data Security Standard (PCI-DSS) and System and Organization Controls 2 [e.g., (SOC 2). DOT expects that these best practices will primarily address user payment methods to protect credit card information. The Plan must also address how the Provider plans to prevent and respond to cyberattacks, including:

- Process for keeping software up to date;
- Monitoring systems and networks for malicious activity;
- Use of secure uniform resource locators (URLs)
- Employee education and training;
- Who is responsible for reporting the attack to the appropriate authorities;
- How customers and others will be alerted;
- How Provider will discover what data and what kind of data was stolen;
- How the Provider will comply with CA Senate Bill 34; and
- Changing and strengthening passwords.

1. Purpose

The City of Oakland Department of Transportation (DOT) intends to enter into an agreement with six selected Providers whose services permit individuals to pay for parking sessions through a mobile phone application (app), website, or text message in Oakland. The six Providers are:

- PayByPhone US Inc. (PayByPhone),
- Passport, Inc. (Passport),
- ParkMobile, LLC (ParkMobile),
- HonkMobile USA Ltd. (Honk),

- Marina Security Services, Inc. and Mortimer Smythe LLC (Oakland Parking Solutions), and
- IPS Group, Inc. (IPS).

Agreements with each of these Providers will permit individuals in Oakland to pay for their parking sessions with Providers' services and in turn, share Parking Data and other relevant data connected with the service and Unprocessed Anonymized Data with DOT through online portals. All six Providers will comply with the City's Surveillance Technology Ordinance, including the approved use policy and impact report for this system, per the future revised agreement and scope of services (see **Appendix A**). Providers will process Raw Parking Payment Transaction Data collected in Oakland to show the following fields in the portal regarding parking sessions:

- Parker license plate (note: this data is necessary for DOT staff in the Parking Citation Assistance Center to respond to citation disputes)
- Transaction date
- Start and stop times
- User fee charged
- Parking (meter) fee charged
- Numerical zone corresponding to parking block

Per the requirements in the "City Data Addendum" to the standard professional services agreement (see **Attachment A**), Providers will maintain their respective online system portal/back-office systems with **none** of the following information visible to City staff at any time for any reason:

- Personally identifiable information (PII), including but not limited to, name, phone number, home address, email address, credit card information and user account details

Oakland is implementing "demand-responsive" parking areas in which parking fees may vary by block in order to reflect demand. So far, this has been limited to the Montclair business District and Chinatown, but will be expanded to all of Oakland's business districts. In these areas, each block has a unique "zone" number. In these demand-responsive areas, zones will correspond to a City-provided Facility ID. This ID will be printed on new parking signs and will not differ by Provider. In all other metered parking areas prior to demand-responsive rates being implemented, the Provider-created ID per block will be used. When choosing to pay by app, customers must enter the zone number with the Provider's platform. Zones are shown in Providers' apps and on signs.

DOT is procuring a multi-provider mobile parking payment (pay by app) system in order to increase the convenience of this service to parkers, enhance data privacy and security components of the system, promote the use of this contactless payment method through a City-branded system, and more holistically support the active management of the parking system. A key improvement will be City of Oakland-branded signs in the public right of way

(PROW) that will direct parkers to a webpage (oaklandca.gov/oakparkplus) with all available Providers, their transaction fees, and promotions. New City-branded signs will first be installed in Montclair and Chinatown before being installed in other metered areas. Parking meters are primarily located in commercial districts where demand for curbside spaces is highest.

By allowing multiple providers to operate in Oakland, visitors will likely not need to download any additional apps and share their information with another provider; rather, they are more likely to be able to use an existing app on their phone and conveniently pay for their parking session. They may also "shop around" among the six Providers to choose a Provider that best suits their needs based on promotions, transaction fees, registration requirements, and privacy policies. Providing more choices to parkers in Oakland may also minimize the number of Providers with whom users, especially visitors to Oakland, must share their information to access this payment option. providers may compete for long-term customers with lower user fees and promotions, and from new community engagement requirements intended to make Providers' services more equitable and inclusive.

DOT receives Unprocessed Anonymized Data to reconcile parking payments, to enforce parking restrictions, such as time limits and meter payments, and to review citation disputes. License plate information is particularly critical to staff issuing citations and processing disputed citations. In receiving Unprocessed Anonymized Data, DOT can confirm that parking rates are accurately charged to parkers, that the City receives accurate parking payments, particularly from parkers in demand-responsive parking program areas, and that citations were issued correctly, in the event that a parking citation is contested over an active mobile payment session. For example, in demand-responsive areas, meter rates change by time of day and block; if staff could not see the zones in transaction data, DOT would not be able to program these specific areas' rates or confirm the accuracy of Providers' rates or revenues in reconciliations and audits. Outside the portal, DOT staff's parking data analyses may summarize this data by zone, date, hour, transaction type, parking duration, or amount. When summarizing by zone (location), staff will use Census blocks for spatial analyses.

The City receives Aggregated Anonymized Data (which does not include license plates) from Providers in order to analyze parking revenues and demand. These uses ultimately inform parking policies and practices that support the City's Parking Principles (Resolution No. 84664 CMS) and shape a more equitable mobility system. Notably, parkers are not and will not be required to use the mobile parking payment system in on- or off-street facilities in Oakland, as the California Vehicle Code requires a physical payment option.[1] As noted above, user account details containing PII will not be visible to City staff in each of the Providers' portals. This data is not necessary to City staff's management or enforcement of the parking system and thus, will not be displayed in the portal.

2. Authorized Use

[1] California Vehicle Code Section 22508.5(d) is available online here: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=VEH&sectionNum=22508.5

Only designated DOT and Finance Department staff will have access to the most recent year of Unprocessed Anonymized Data received from Providers through unique portal credentials. Specific applications of mobile parking payment data that supports this effort will include only the following:

a) Reconciling payment transactions with total parking revenues received
b) Promoting compliance and enforcing parking restrictions, permits, and payment
c) Reviewing contested parking citations
d) Remitting user transaction fees to Providers via invoices

Designated DOT and Finance Department staff will also have access to Aggregated Anonymized Data received from Providers through unique portal credentials. Use of this data (which exclude PII and are unable to be re-identified) may include, but is not limited to, the following:

e) Estimating parking demand, occupancy, and revenues by block face
f) Evaluating parking payment options
g) Monitoring demand-responsive parking areas and general levels of compliance with parking rules

DOT staff may use Aggregated Anonymized Data in public reports, post it to the City's open data portal or otherwise make it available for public use.

3. Data Collection

Mobile parking payment users generate Parking Data by making transactions for parking. Providers collect Raw Parking Payment Transaction Data from these transactions and push Unprocessed Anonymized Data and Aggregated Anonymized Data to their portal for DOT and Finance staff to view. As stated in Section 1, Unprocessed Anonymized Data will never include PII. Rather, this dataset will include parking date and start and end times for each transaction, payment amounts, transaction fees for the Providers, and numbered "zones" corresponding to parking location.

The Providers must collect Raw Parking Payment Transaction Data in order to process financial transactions in compliance with their System Security Plan, including Payment Card Industry Data Security Standard (PCI-DSS), System and Organization Controls 2 (SOC 2), and Senate Bill No. 34. All six selected Providers currently maintain PCI-DSS and SOC 2 compliance and must continue to do so.

4. Data Access

Only authorized staff from the DOT and the City's Finance Department will have access to the most recent year of Unprocessed Anonymized Data. Data will be accessed through Providers'

online platforms. Authorized users of the online platforms will require a unique username and password. Because all data in the platform will have no personally identifiable information or individual user account information, any data shared outside the platform, such as through public records requests, court orders, or in the City's Open Data Portal, will be anonymous, thus prohibiting City staff from identifying individuals from this parking data. Anyone can have access to the Aggregated Anonymized Data. Staff may upload Aggregated Anonymized Data to the City's open data portal for easier public access.

5. Data Protection

DOT will depend on each Provider to securely store, transmit, and audit transaction and user data per requirements in their Scope of Services and per industry best practices. Providers will also be required to provide a System Security Plan with data security, storage, and encryption practices that meet or exceed industry standards, including Payment Card Industry Data Security Standard (PCI-DSS) and System and Organization Controls 2 [e.g., (SOC 2). All six Providers comply with PCI-DSS and SOC 2 standards at a level corresponding to their number of annual transactions processed. DOT expects that these best practices will primarily address user payment methods to protect credit card information.

Five of six Providers also have existing user terms and conditions and privacy policies available for their services (see **Appendix B** and **Appendix C**). Only Oakland Parking Solutions, a local company that is custom-building an app for Oakland, does not have these documents available for review yet.

However, all Providers, including Oakland Parking Solutions, will be required to accept and comply with the "City Data Addendum" to the professional services agreement (see Attachment A), including the approved use policy and impact report for this system, upon the signing of their respective agreements. DOT also requires that every Provider has a secure gateway service for secure (encrypted) credit card data transmission to the City's merchant account Provider.

DOT staff worked with the Capital Contracts Division and the City Attorney's Office to include the requirement to comply with the approved Use Policy and Impact Report for this system in the Provider's Professional Services Agreement. By situating this requirement in the body of that agreement, in addition to the scope of services (see **Appendix A**), the City will have greater capability to enforce this requirement in the event of non-compliance. The existing agreement language, as edited by the City Attorney's Office, can be found in **Appendix D**.

6. Data Retention

Under the existing agreement with ParkMobile, the precedent for retaining mobile parking payment data in their portal is two (2) years. However, staff will reduce this requirement to one (1) year. At least one year is needed in order to provide sufficient time for parking citation appeal processes.

Raw Parking Payment Transaction Data is unaggregated, unsummarized data for each parking event. Providers will store all Raw Parking Payment Transaction Data collected in Oakland for no more than one (1) year. If the contract between a Provider and DOT is severed, the Provider will be required, per the signed Professional Services Agreement, to delete all Raw Parking Payment Transaction Data collected in Oakland (see **Appendix A**). If such contract severance occurs, the Provider will email the DOT Project Manager, within 30 days of contract severance, a confirmation that all raw data collected in Oakland has been deleted.

Unprocessed Anonymized Data Includes parking transaction date with start and stop times for each transaction, meter payment amounts, user transaction fees charged by the Providers, and numbered “zones” corresponding to parking location. Unprocessed Anonymized Data does not contain any data on the customer except for the vehicle’s license plate number. This data will be stored by Providers and the City for no more than one (1) year.

Aggregated Anonymized Data is a processed version of Unprocessed Anonymized Data that does not include any data on individual transactions. It contains only a sum of the total number of transactions that occurred on each block face during each one-hour period of each day and the total revenue received from the sum of those transactions. This data is important for staff to examine long-term trends in parking occupancy and revenue. If the contract between a Provider and DOT is severed, the Provider will be required per the signed agreement to delete all Aggregated Anonymized Data generated in Oakland. The City may retain this data indefinitely.

Staff currently do not have access to any Parkmobile user account information and will continue to not have this access to protect user privacy. With multiple providers now competing for Oakland parkers’ payments, staff will not ask ParkMobile to migrate user information or data to any of the new Providers operating under the upcoming mobile parking payment system. Parkers may continue to use ParkMobile in Oakland, or any other selected Provider’s app of their choosing.

7. Public Access

The public may access the Aggregated Anonymized Data provided in each Provider’s portal through public records requests. Aggregated Anonymized Data may also be added to the City’s Open Data Portal. Raw Parking Payment Transaction Data and Unprocessed Anonymized Data will only be released as required by law under subpoenas, warrants, or other court orders.

8. Third-Party Data-Sharing

Providers collect and generate Parking Data associated with the mobile parking payment system. Providing only Unprocessed Anonymized Data and Aggregated Anonymized Data in the portal that Providers give to City staff (removing PII) reduces the risk of surveillance and eliminates the possibility of user identification by City staff. However, staff understand that a primary concern is the security of the Third Party Data Contractors that Providers use, particularly following the ParkMobile data breach in March 2021.

Providers may contract with Third Party Data Contractors to process and/or store data. If using Third Party Data Contractors, Providers must:

- Mandate to any Third Party Data Contractors that they follow the same System Security Plan terms as the Providers; and
- Only provide access to Unprocessed Anonymized Data and/or Aggregated Anonymized Data; and
- Disclose to users, in the Providers' privacy policies, what data is shared with third parties (see **Appendix B**).

Providers may not share or sell Parking Data collected in Oakland with any third parties except for:

- Third Party Data Contractors that are contracted with for legitimate and necessary data services such as data storage and processing and subject to the terms listed above; and
- Aggregated Anonymized Data.

Notably, DOT does not have the capacity or means to create a mobile parking payment service in-house specific to Oakland parkers and is thus reliant on the selected Providers' services. Because working with third parties to securely store data is a widespread industry practice, staff believe that Providers are in a similar position – they do not have the capacity or means to securely process and/or store millions of parking transaction data in-house.

9. Training

Each Provider is required to provide web-based or on-site training for authorized City staff in the DOT Parking & Mobility Division, the Finance Department, or both (see **Appendix A**).

10. Audit and Oversight

As shown in the draft Professional Services Agreement scope (see **Appendix A**), all six selected Providers are required to provide a fully auditable mobile parking payment service. DOT or Finance staff will audit Providers through their respective back-end online data portals, in addition to Providers going through PCI DSS audits and any other audits that Providers have independently arranged. Audits by DOT or Finance staff will occur on an as-needed basis, such as audits of a sub-set of zones where meter rates were recently changed. General oversight of the Providers are the responsibility of the Parking & Mobility Division Manager. The legally enforceable sanctions for violations of the policy include relevant administrative instructions as well as provisions in the Surveillance and Community Safety Ordinance.

11. Maintenance

Providers are responsible for maintaining and managing all data generated through their respective app, website, and text message services. As noted in the Third-Party Data-Sharing

section of this report, Third Party Data Contractors are generally used by Providers for storage and/or security purposes.

Questions or comments concerning this draft Use Policy should be directed to Michael Ford, Division Manager, Parking and Mobility Division, via email at mford@oaklandca.gov or phone at (510) 238-7670.

ATTACHMENT A

DRAFT – CITY DATA ADDENDUM

This City Data Addendum [”Addendum”] is Exhibit 1 to the Professional Services Agreement between the City of Oakland [“City”] and [VENDOR’S NAME] [“Contractor”] to provide Mobile Parking Payment Services [“Agreement”] as is set forth with specificity therein and is incorporated into the Agreement by this reference. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms of this Addendum shall prevail but only with respect to the matters stated herein.

1. Background

As is set forth with specificity in the Agreement’s Statement of Work Exhibit [INSERT CITATION], Contractor avers and covenants to develop, implement and operate a mobile parking payment system [“System”] that, at a minimum, will enable customers to remotely pay for parking sessions by using mobile phones or mobile devices to provide Contractor payment information which Contractor will collect and store for City on Contractor’s mobile software application, website, and/or phone number for City-controlled paid parking [“Services”]. Contractor’s Services may also support daily or monthly permits by zone merchant validation

Given the sensitive nature of the information Contractor will collect and store for City, Contractor further avers and covenants that its System and Services will meet the City’s key goal of enhancing user data protections by complying with: (1) the City’s Surveillance Technology Ordinance (Oakland Municipal Code Chapter 9.64); (2) the City’s Surveillance Impact Report [Exhibit INSERT]; and, (3) the City’s Mobile Parking Payment Use Policy [Exhibit INSERT], all of which are incorporated herein by this reference.

ATTACHMENT A

2. Information to be Collected

The Agreement will require Contractor to collect from the users of its System, a broad range of personal and sensitive information. The California Consumer Privacy Act [CCPA][1] and Consumer Privacy Rights Act ["CPRA"] [2] definitions for "personal information"[3] and "sensitive personal information"[4] are incorporated herein by this reference and shall apply to the information Contractor collects.

3. Ownership of Information Contractor Collects

With the exception of that information which is publicly known or available as set forth in Section [INSERT] ["Confidential Information"] of the Agreement, all data, files, documentation, information, communications, media, whether intangible or tangible, whether provided directly or indirectly by Contractor to provide its Services, together with any and all results of Contractor's providing of its Services, including all data Contractor accesses , collects, modifies, develops as work product, or otherwise generates while providing its Services to City under this Agreement, whether pursuant or incidental to the purposes of the Agreement and whether or not delivered to the City, shall be the exclusive property of, and all ownership rights therein shall vest in, the City (collectively "City Data").

To the extent necessary, Contractor hereby assigns to the City, the rights to City Data which arise out of, or are developed in connection with or are the results of, Contractor's Services.

---

[1] Cal. Civ. Code Section 1798 *et. seq.*

[2] The CPRA is more accurately described as an amendment of the CCPA. The CPRA specifically states that it "amends" existing provisions of Title 1.81.5 of the California Civil Code (currently known as the CCPA) and "adds" new provisions (related to the establishment of the California Privacy Protection Agency).

[3] It identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

[4] It contains some or all of the following;

- social security, driver's license, state identification card, or passport number
- account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

4. Use of City Data

4.1 By Contractor

Contractor avers and covenants to:

- Comply with the terms of the City's Surveillance Technology Ordinance [OMC 9.64]
- Comply with
    - the City's Surveillance Impact Report [Exhibit INSERT CITATION];
    - the City's Mobile Parking Payment Use Policy [Exhibit INSERT CITATION],
- Anonymize the City Data and take such other steps as may be required to assure that personally identifiable or personally sensitive information are not visible to City staff at any time for any reason;
- Not sell rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, City Data, to another business or a third party for monetary or other valuable consideration;
- Only share City Data with third parties as permitted by City's Mobile Parking Payment Use Policy [Exhibit INSERT CITATION; Section 8 "Third-Party Data-Sharing"];
- Only use City Data to fulfill its obligations to City under the Agreement;
- Comply with the terms of the Agreement;
- Implement security safeguards;
- Not combine City Data with personal information received from others;
- Notify City when it uses subcontractors;
- Pass through the Agreement's terms and conditions to any subcontractors it uses;

.

Contractor shall fully indemnify City for any third-party claims against City resulting from Contractor's use of City Data in violation of this Addendum's provisions.

3.2 By City

City's access to City Data shall be limited to authorized staff and used only as permitted by City's Surveillance Use Policy [INSERT CITATION] and as required by City's parking enforcement responsibilities [INSERT CITATION]] which include but, are not limited to, shaping parking policies and practices to better support the City's Parking Principles and developing a more equitable mobility system. In this regard, only designated DOT and Finance Department staff will have access through unique portal credentials to the following *anonymized* City Data Contractor stores:

- Estimating parking demand, occupancy, and revenues;
- Evaluating parking payment options;
- Monitoring demand-responsive parking areas and compliance;
- Reconciling payment transactions with total parking revenues received;
- Promoting compliance and enforcing parking restrictions, permits, and payment;
- Reviewing contested parking citations;
- Remitting user transaction fees to Providers via invoices;

4. Contractor's System Security

This Agreement requires Contractor to store City Data in Contractor's certified data center[s] which are external to the City's premises and administered by Contractor for the purposes of this Agreement ["System"]. City's Data is highly sensitive, confidential and is of paramount importance to the City because unauthorized disclosures of the Data could seriously harm the City and possibly third parties.

Contractor acknowledges that City, in entering into this Agreement with Contractor, is relying upon Contractor's professional expertise, know-how, judgment, experience and its

representations in its System Security Plan [INSERT CITE TO VENDOR'S PLAN] that the integrity of the security, availability and processing of its System protects and preserves the confidentiality and privacy of the City Data. Contractor warrants that its System has been accredited under industry recognized standards [e.g., SOC 2] and that, at all times, Contractor will maintain and ensure that the Data remains secure and does not through any of Contractor's actions or lack of action thereof become vulnerable to unauthorized access by third parties.

Contractor avers and covenants to continue to take all technical and organizational measures necessary to protect the information technology systems and data used in connection with the operation of the Contractor's business. Without limiting the foregoing, Contractor will continue to use reasonable efforts to establish and maintain, implement and comply with, reasonable information technology, information security, cyber security and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or data used in connection with the operation of Contractor's business.

Contractor agrees to maintain the City Data and to not disclose such information except as required to perform hereunder or as required by law.. Contractor shall maintain network risk and cyber liability coverage (including coverage for unauthorized access, failure of security, breach of privacy perils, as well at notification costs and regulatory defense) as required by the City's Schedule Q. Such insurance shall be maintained in force at all times during the term of this Agreement

Notwithstanding as may be otherwise provided in either this Addendum or this Agreement and, with the exception of those instances for which the City is responsible,

Contractor avers and covenants to be solely responsible for restoring and correcting any corruption to City's Data that occur by reason of Contractor's actions or lack thereof, including ransomware attacks upon Contractor and to fully indemnify the City for any claims against City and injury to City resulting from corruptions of the City Data.

5. DATA INCIDENTS

a. Contractor shall be responsible for managing the correction of unauthorized disclosure of, access to, or use of any City Data however they may occur ("Data Incidents").

b. 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.

c. 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 (i) compensate City for any reasonable expense related to notification of consumers and (ii) provide 2 years of credit monitoring service to any affected individual.

d. 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 [INSERT CITATION TO CONFIDENTIAL INFORMATION OF THE CONTRACT WITH THE VENDOR] Contractor is not required to give City access to records that might compromise the security of Contractor's other users. City will coordinate with Contractor on the content of any intended public statements or required

notices for the affected individuals and/or notices to the relevant authorities regarding the Data Incident(s).

6. Termination of the Agreement

Within ten (10) days of the date of termination of the Agreement for any reason, Contractor shall send all City Data to City in a format acceptable to the City and which protects and preserves the sensitive nature of the City Data. Contractor may not keep copies of the City Data. For the purposes of this provision, Contractor's Assignment of the Agreement under Section [INSERT CITATION] ["Assignment"] or Bankruptcy under Section [INSERT CITATION] ["Bankruptcy"] of the Agreement or cessation of business shall be considered a Termination of the Agreement.

Exhibit 1

STATEMENT OF WORK

The Contractor will be expected to provide the development, implementation, and operation of a mobile parking payment system services that, at minimum, would enable customers to remotely pay for parking sessions using mobile phones or mobile devices through the Contractor's mobile software application, website, and/or phone number for City-controlled paid parking. The City is also seeking, but is not requiring, services that support special permits (daily or monthly permits by zone) and merchant validation.

The mobile parking payment system provided by the Contractor shall be fully interfaced with the City's existing enforcement and citation management systems. The City's Parking Control Technicians must be able to view valid parking sessions made with the Contractor through their handheld devices. In demand-responsive parking areas of Oakland, the corresponding zone number must be visible in Parking Control Technicians' handhelds. In the case of an errant citation, the City must be able to check if parking sessions made through the Contractor's system have approved payment methods. Upon approval through the Contractor's system, valid parking session payment made through the Contractor must be received by the City and its financial system. All parking fees, including system and user fees, will be deposited into the City's bank account, then reimbursed to the Contractor.

The term of the awarded Agreement shall be for a base term of five (5) years, with two (2) consecutive one-year options to extend the term of the Agreement at the City's sole discretion. The mobile parking payment system(s) must be fully developed, implemented, and operational on the date specified in the awarded Agreement. Contractor shall be permitted to charge customers a single flat convenience/user fee per transaction for each use of the service. The convenience/user fee amount shall be approved in writing by the City. The City reserves the right to subsidize this convenience/user fee at any time during this agreement's duration. After the five-year base term of the agreement, selected Contractor(s) may request changes to the convenience/user fee amount. This request must be submitted in writing to the City of Oakland project manager or designated representative 90 calendar days prior to taking effect. The City of Oakland reserves the right to refuse a change to a Contractor(s)' requested change(s) to the convenience/user fee amount. Any changes to the convenience/use fee amount must be approved in writing by the City of Oakland in order for those changes to take effect.

The successful Contractor(s) shall have the appropriate professional and technical background as well as access to adequate resources to fulfill the statement of work, as outlined in Tasks 1 and 2 below. The City may select multiple qualified Contractors for the mobile parking payment system (Task 1). Contractor(s) may also choose to respond to Task 2 if the Contractor has additional services or products that can effectively support the on-street and off-street parking system.

TASK 1 Mobile Parking Payment System

1.1 Technical Requirements and System Integration. The system must perform key technical functions and have full integration capabilities with the City's existing systems. The following system requirements must be met at no cost to the City of Oakland, as only the convenience/user fees applied be invoiced by the awarded Contractor(s):

- Integrate with the City's current parking citation processing system (Conduent's eTIMS®) and accommodate any future potential changes to the system.
- Integrate with current parking enforcement handhelds (Zebra TC75X) and Automated License Plate Readers (Genetech's AutoVu) and accommodate any future potential changes to parking enforcement equipment.
  - For context, City of Oakland Parking Control Technicians conduct enforcement queries by zone up front and double check for payment at the end of the ticket-writing transaction to confirm a payment has been made.
- Integrate with digital payment technology and IPS single- and multi-space meters, should the City decide to "push" mobile payments to meters.
- Integrate with any other parking data, payment, and management systems and platforms that the City may acquire during the Contractor(s) operation.
- Display the status of paid vehicles on any Internet browser, in real time, through a secure portal requiring unique credentials for each staff member with access.
- Provide the ability to cross-reference transactions between vehicles, individual meters, streets, block, zone, or other designated identifiers.
- Provide the ability to geographically depict/map parking transaction activity.
- Provide real-time transaction information in the form of printable reports (such as through an online portal/back-office system) and accessible through enforcement handheld devices for purposes of enforcement and verification/audit of real-time push to IPS smart meters.
- Integrate payment zones with the City's selected number typology.
- Provide the capability for the City, instead of parkers, to pay transaction fees on an as-needed basis, such as for a district-specific holiday promotion.
  - This capability should include a pop-up or notification to customers that the City of Oakland is covering user fees. Contractor(s) shall be able to provide this capability citywide or in specific zones upon the City's request and may recommend zones/districts where this promotion would be beneficial to parkers, such as where there is low mobile parking payment adoption.

1.2 Point of Service: The system must provide key points of service to parking customers. The system must allow customers to perform the following functions:

- Create an account/register via mobile smartphone app, over the phone through an automated system, and over the Internet via mobile and desktop web with minimal input requirements (basic information) and be able to immediately begin using the account.
- Other registration options/platforms are encouraged but not required (Facebook,

etc.).

- Start a parking transaction and make payment via smartphone software application, Interactive Voice Response (IVR), Short Message Service (SMS), or website.
- Be alerted automatically via text prior to a parking session expiring.
- Extend a parking session and purchase additional time within established time parameters via smartphone software application, IVR, SMS, or over the internet via mobile and desktop website.
- Extend a parking session without re-entering complete location information.
- Extend a parking session without incurring additional convenience/user fee.
- Initiate a new parking session at a previously parked location without re-entering information.
- Prepay for parking during a designated "prepayment period."

1.3 System Setting Requirements: The system must include unique settings that permit the following functions:

- Utilize and display City-created block ID numbers containing up to eight (8) alphanumeric characters for payment zones.
- Allow settings to vary at each individual meter, by block, by zone, by time, by restriction, and by other custom configurations/groupings.
- Allow custom settings to define and/or modify maximum stay restrictions.
- Allow the programming of multiple, custom, and variable rate structures by time of day, day of week, hours of operation, length of stay, by individual meter, by zone, and by other custom configurations/groupings.
- Allow custom, unlimited configuration changes related to rates, hours of operation, and time limits to be programmed in advance with the ability to be active within two (2) days of the programming change. All other system configuration changes/updates shall be made within five (5) days of notification.
- Have the ability for Contractor to change parking session rates to support the City's demand-responsive parking program. Contractor should specify in how many business days they are able to adjust rates and for rates to be available with the system.
- Disallow parking transactions to be initiated on City designated holidays or during periods designated by the City as no parking.
- Allow for custom grouping of meters to facilitate enforcement, revenue reporting, and demand-responsive parking rate programming.
- Enable City staff to add, remove, or alter meters or spaces within the pay-by-phone system inventory.
- Allow for the deactivation or suspension of a customer account in the event that a parking payment transaction is declined three (3) times and provide notification to customer of such action.
- Allow City staff to access up to two (2) years of data in the Contractor's online portal/back-office system.
    - If the contract between the Contractor and DOT is severed, the Contractor will be required to delete all raw parking payment transaction data collected in Oakland.

- Provide an online system portal/back-office system that includes parking date and start and end times, payment amounts, transaction fees for the Providers, and numbered "zones" corresponding to parking location.
- Incorporate the latest Americans with Disabilities Act (ADA) Guidelines and best practices for accessible digital content, including but not limited to Section 508.

1.4 Data Privacy Requirements: One of the key goals of this new pay-by-phone system is to enhance user data protections. The system must comply with the City's Surveillance Technology Ordinance (Oakland Municipal Code Chapter 9.64) and subsequent system use policy and anticipated impact report[1] in the following capacities:

- Maintain an online system portal/back-office system with **none** of the following information visible to staff at any time for any reason:
  - Personally identifiable information (PII), such as phone number and email address
  - Customer license plate information (note: this information must be visible for real-time enforcement purposes, but not to office staff accessing the online portal)
  - Individual user account details
- Provide a system with data security, storage, and encryption practices that meet or exceed industry standards. DOT expects that these best practices will primarily address user payment methods to protect credit card information.
- Disclose any additional companies who would support the Contractor's system, such as third-party cloud storage services.
- Ensure the security of user and transaction data through security protocols per current industry standards.
- Provide a data storage and privacy system that meets or exceeds industry standards. Contractor must comply with the City's Surveillance and Community Safety Ordinance (Oakland Municipal Code Chapter 9.64), the approved policy use regarding the mobile parking payment system, and any other relevant surveillance laws relevant to Oakland, California.

1.5 Customer Base System Requirements: The system must support customer transactions and should provide a positive customer experience. The system must allow the following functions:

- Provide a toll-free live customer service telephone support for all aspects of the pay-by-phone system.
- Allow customers the option to transfer to a live customer service agent at any time when utilizing an automated system.

[1] These documents will be made available on the City's website:

oaklandca.gov/topics/approved-impact-reports-and-use-policies

- Allow customers the ability to manage, modify and track account details, update settings and profile, review usage, view transactions, and print receipts via the smartphone software application and over the internet via mobile and desktop web.
- Allow customers the ability to designate multiple vehicle license plates to a single account.
- Provide customers email receipts of all parking transactions.

1.6 Payment System Settings: The system must permit the following functions to support customer payments, parking system management, and parking payment reconciliation and audits:

- Include all applicable convenience/user fees assessed to users.
- Notify customer of any convenience/user fees to be charged regardless of payment type/option utilized.
- Provide revenue, utilization, and other reports in a format exportable to Excel, allowing for easy data analysis, record keeping/documentation, and reconciliation.
- Provide a secure gateway service for secure (encrypted) credit card data transmission to the City's merchant account provider. Credit card data transmission shall meet the Payment Card Industry Data Security Standards (PCI DSS) Level 1 certification.
- Authorize payments in real time and accept payment through Visa, MasterCard, Discover, American Express, all debit cards, and other alternate payment methods (i.e. PayPal, Apple Pay, Google Pay, Venmo, etc.).
- Document for review and report rejected/declined transactions to the customer.
- Provide a single opportunity for customers to try a different credit or debit card when a rejected transaction occurs.
- Ensure declined transactions are not incorrectly posted within the revenue reporting system or pushed to the meter.
- Synchronize batch settlement times for the merchant account and report of the same sent via the Internet to the City.
- Have expansion capacity and state how much expansion capacity the system has in terms of spaces, meters, or any other defined criteria.
- Have the capability to implement parking validation, such as allowing merchants to generate and provide customers with unique discount codes.
- Provide a fully auditable service and online portal/back-office system for as-needed audits conducted by City staff, in addition to complying with PCI DSS audits.

1.7 Informational Materials and Promotion: The system must include informational materials and the promotion of the City's integrated mobile parking payment system, such as through the use of stickers, decals, and/or signage and online promotions. All materials in the public right-of-way will be Oakland-branded and connect parkers to an Oakland-branded website. The website will direct parkers to all permitted Contractors, such as by showing individual Contractor logos and links to their platforms.

While the City will install and maintain informational materials, such as City-branded parking signs, in the public right-of-way, Contractor(s) shall pay for the cost of these activities through both an initial fee and ongoing revenue sharing of user/transaction fees paid to the City. The City is committed to promoting the use of this new system and is seeking financial support from Contractor(s) to fully execute this commitment and ensure Oakland parkers' access to their services.

The City is seeking an initial one-time combined payment of $190,000 from all selected Contractor(s) to contribute to the costs of establishing the new mobile parking payment system. $190,000 shall be divided equally between all selected Contractor(s), unless otherwise specified or unless the Contractor(s) is a certified LBE. If the Contractor(s) is a certified LBE, then this Contractor(s) shall contribute 75% of their divided portion.

Unless otherwise determined in negotiation, selected Contractor(s) shall pay: 1) their agreed-upon portion of $190,000 one-time fee to the City at the beginning of the agreement term and 2) 10% of all convenience/user fees collected shall be kept by the City of Oakland.

The system must include the following materials and promotion:

- Contribute toward the cost to install City-branded signage for paid parking areas. Contractor must propose a certain annual percentage of transaction, user, and/or gateway fees that they will commit to a City account dedicated to installing, maintaining, and replacing parking signs, stickers, and/or decals.
- Provide funding for Oakland-branded materials to promote the mobile parking payment system that will be displayed in the public right-of-way and online. Materials shall include but are not limited to signs, stickers, and decals.
  - Materials must show individual zone numbers and a link to the City's website page on available mobile parking payment system(s). City will approve final stickers, decals, and signs prior to the Contractor's' installation.
  - Signage proposals shall meet the City's requirements/specifications for signage design, manufacturing, and maintenance.
- Support City staff in connecting parkers to the Contractor's product on the City's online Oakland-branded platform. Support may include but is not limited to links that open Contractor's smartphone software applications or website and official Contractor logos provided as .png or .jpg images.
  - Provide City staff with digital informational or marketing materials, such as promotions to include on the City's mobile parking payment system website (e.g., a digital coupon code for new sign-ups on the Contractor's app) and instructions on how to use the Contractor's product.

1.8 System Set-up and Training: The system set-up shall be without cost to the City and must include but not be limited to the following functions:

- Supply reports for account sign-up and use, customer service issues, revenue, and

additional reports deemed necessary by the City to properly evaluate program progress.
- Describe reporting options in their response including whether reports can be customized.
- Provide on-site or web-based training and manuals for the authorized City personnel to navigate and utilize the online portal/back-office system.

1.9 Community Benefit and Engagement: Contractor(s) staff shall maximize the benefits of their pay-by-phone system to Oakland parkers by engaging directly with community members and organizations. Methods of engagement will include, but not be limited to, the following:

- Attend up to four (4) community events per year either in-person or virtual, such as business improvement district (BID) meetings, Oakland City Council or commission meetings, and neighborhood events.
  - Two (2) or more of these events must occur in Equity Priority Communities, as defined by the Metropolitan Transportation Commission, as shown here: https://mtc.maps.arcgis.com/apps/mapviewer/index.html?layers=28a03a46fe9c4df0a29746d6f8c633c8
- Incorporate community feedback into Contractor's product functionalities, promotions, marketing materials, and system.
- Align Contractor's goals for their product in Oakland with community goals, such as goals formed in the Contractor's collaboration and outreach with community members and goals stated in OakDOT plans to promote a sustainable, equitable and livable city.

Task 1 Deliverables:

- *Fully integrated and set-up parking payment system that meets all technical requirements, permits all points of service to the public, meets setting and customer base requirements, includes all payment system settings, and provides informational materials and promotion.*
  - *Informational materials and promotion including but not limited to stickers, decals, and signage installation.*
  - *Web-based trainings and manuals for authorized City personnel to navigate and utilize the online portal/back-office system.*
- *Attendance and support at up to four (4) community events per year, either in-person or virtual.*

TASK 2 (OPTIONAL) Additional Parking System Support

In addition to providing a mobile parking payment system, Contractor(s) may choose to include additional innovative products or services for the City's consideration. These products or

services should support the active management of the City's parking system, supporting access to commercial areas and curbside spaces, and integrating off-street facilities into the City's on-street system.

Task 2 Deliverables:

- *Innovative product(s) or service(s) that supports the parking system.*
    - *Examples of such products or services may include: pay-by-text parking payment, gateless parking system technologies, integrated pay-by-phone services for Contractor(s), commercial vehicle parking permits, integrated enforcement features, and equitable cash payment alternatives.*
    - *Product or service should include detailed pricing, technical requirements, named benefits to Oakland's parking system, other municipalities or organizations where the product or service is in use, and any other relevant information.*

2. DELIVERABLES

Deliverables listed below shall be provided to the City per a timeline agreed upon by City and the Contractor. Request for information or reports shall be fulfilled by the Contractor within three (3) business days of the request.

Task 1 Deliverables:

- *Fully integrated and set-up parking payment system that meets all technical requirements, permits all points of service to the public, meets setting and customer base requirements, includes all payment system settings, and provides informational materials and promotion.*
    - *Informational materials and promotion including but not limited to stickers, decals, and signage installation.*
    - *Web-based trainings and manuals for authorized City personnel to navigate and utilize the online portal/back-office system.*
- *Attendance and support at up to four (4) community events per year, either in-person or virtual.*

Task 2 Deliverables:

- *Innovative product(s) or service(s) that supports the parking system.*
    - *Examples of such products or services include: pay-by-text parking payment, gateless parking system technologies, and equitable cash payment alternatives.*
    - *Product or service should include detailed pricing, technical requirements, named benefits to Oakland's parking system, other municipalities or organizations where the product or service is in use, and any other relevant information.*

DRAFT

PROPOSED USE POLICY FOR VEHICLE-MOUNTED AUTOMATED LICENSE PLATE RECOGNITION (APLR) FOR PARKING MANAGEMENT AND ENFORCEMENT

Michael P. Ford, Ph.D.
Acting Manager
Parking and Mobility Division
Department of Transportation
City of Oakland

May 1, 2018

1. Purpose

Vehicle-mounted Automated License Plate Recognition (ALPR**)** technology shall be used to automate the processing of vehicle license plate information by transforming images into alphanumeric characters with optical recognition software and storing those images, plate information and related metadata, including time and geo-location information. City of Oakland staff propose to use ALPR for parking management and enforcement purposes.

[**Note**: The purpose of this draft Use Policy, together with the accompanying draft Impact Assessment report and attachments, is to seek input and guidance from the Privacy Advisory Commission in the Department of Transportation's efforts to develop a robust policy that helps the City realize all the benefits of its investments in ALPR for parking operations, while safeguarding the civil liberties and privacy of the community.

In support of this effort, staff have attached ALPR reports and policies from the Cities of Berkeley and Sacramento, which staff view as examples of recent and possibly best practices in this area. Staff request that the Privacy Commission consider highlighting language in those examples that it finds either exemplary or problematic.

Also, in drafting this and the accompanying Impact Assessment, one question repeatedly came to mind: What kind and amount of detail from third-party vendors such as Conduent, the City's Parking Citation system supplier, can/should staff provide in its efforts to satisfy the requirements of the new Surveillance and Committee Safety Ordinance? Conduent's winning proposal to the recently completed competitive request for Parking Citation system proposals is attached as an example of such details.]

2. Authorized Use

Authorized uses of ALPR technology include:

- "Virtual chalk," automating the time-stamping of vehicles in time-limited

parking spaces and areas;

- "Digital permits," including annual, weekly, and other limited-duration permits in parking privilege permit areas, e.g., Residential Permit Parking (RPP) areas;
- Parking payment verification, including "pay-by-phone" and "pay-by-plate";
- "Hotlist" identification, including scofflaw and stolen vehicles;
- Parking demand management, including parking occupancy and turn-over counts and analysis;
- "Smart parking" applications, including mobile apps providing parking availability and wayfinding information.

3. Data Collection

Data collection occurs via vehicle-mounted ALPR through the indiscriminate capture of images as the specially-equipped Parking Enforcement vehicle moves through the right-of-way. Images of vehicle license plates are processed using optical character recognition, time and geo-stamped, and analyzed in real time with the aim of registering potential violations and matching license plates against "hotlists" (as described above). Data is stored on servers secured and administered by the City's third-party Parking Citation system vendor, Conduent.

4. Data Access

Authorized staff may be from the City's Department of Transportation (DOT), Finance Management Bureau (FMB), Oakland Police Department (OPD) or other departments that contribute to the City's parking operations. Procurement and administration of ALPR contracts and systems is the responsibility of the City's Revenue and Tax Administrator in the Revenue Division of the FMB.

5. Data Protection

City staff depend on its vendor, Conduent, to source and administer its ALRP solution. As such, the City is relying on the safeguards to protect ALPR information from unauthorized access through the use of appropriate control mechanisms as provided by Conduent, e.g., user access to and use of the system is controlled and recorded for audit purposes.

6. Data Retention

Again, City staff depend on Conduent to deliver on the data retention requirements of its Parking Citation system. The following has been incorporated into Conduent's scope of services:

- Archive or Purge citation data on an agreed upon schedule or as directed by City Staff.
- Archived data should remain accessible to online inquiry and retrieval as needed.
- Conduent must provide method for access for archived data. Disaster and recovery plans must be provided for this data as well.
- Provide electronic images of citations issued on demand.

- Transfer data in format determined by City Staff as needed.
- Retain all payment documentation for 7 years.

The reason for these requirements is that they meet the City's minimum needs for administering the parking citation administrative process.

7. Public Access

Except where prohibited or limited by law, the public may access ALPR data through public records requests.

8. Third-Party Data-Sharing

The City depends on Conduent and other third-party vendors for a comprehensive parking citation system, e.g., the Conduent system will build a "hot list" of vehicles subject to scofflaw and share this information with Paylock, a vendor contracted with the City since 2009 to provide a "smart parking boot" solution.

Parking occupancy information originating from the ALPR technology may be shared with and used by third-parties for smart parking applications. In such cases, license plate and other identifiable forms of data would be purges, resulting in only anonymous "counts" or "turn-over" indicators with time and geo-spatial information.

9. Training

Training for operating ALPR will be provided by the system vendor and will be limited to authorized City staff. Staff will direct Conduent to incorporate this use policy and related privacy policies and procedures into its training materials.

10. Auditing and Oversight

City staff depend on Conduent to provide a "fully auditable" ALPR solution. For example, with the Conduent system staff expect transactions to be recorded in audit logs that capture the user ID of persons performing transactions, including the date, time and description of the functions performed. General oversight of the system falls to the City's contract manager, currently the Tax and Revenue Administrator. DOT oversight and responsibility for the ALPR solution will fall to the Parking and Mobility Division Manager. The legally enforceable sanctions for violations of the policy include relevant administrative instructions [TBD] as well as provisions in the new Surveillance and Community Safety Ordinance currently before City Council.

11. Maintenance

The City's third-party vendor, Conduent, will be required to maintain the integrity of the Parking Citation system in general and the ALPR solution in particular. Details of the mechanisms and procedures are included in the City's contract.

Questions or comments concerning this draft Use Policy should be directed to Michael Ford, Acting Manager, Parking and Mobility Division, via email at mford@oaklandca.gov or phone at (510) 238-7670.

DEPARTMENTAL GENERAL ORDER

I-29: Fixed-Wing Aircraft Mounted Camera Surveillance Use Policy

Effective Date: DD MMM YY
Coordinator: Special Operations Division

COMMAND INTENT

The Oakland Police Department believes in protecting and serving its diverse community and city through fair, equitable, and constitutional policing. OPD believes in the usage of technology to aid in this mission and in the investment into progressive forms of surveillance technology which both protects the unassailable rights of members of the community, while also ensuring and enhancing the safety of community members, officers, and engaged persons. This includes a multipronged approach related to tactics, methodology, and technology that allows for de-escalation in often rapidly evolving and tumultuous environments.

At the direction of the Oakland City Council, Oakland Public Safety Committee, Reimagining Public Safety Task Force, and the Oakland Police Department, the Air Support Unit has explored numerous alternatives to the current methods and equipment utilized by the Air Unit. After careful consideration, product testing/evaluation, fiscal analysis, stakeholder input, and industry standards, the Department requested that a fixed-wing aircraft be purchased for use by the Air Support Unit. The use of a fixed-wing aircraft necessitates the utilization of an Aircraft Mounted Camera (AMC) which allows a Flight Observer (FO) to observe, document, and relay the events occurring on the ground, to responding officers, partnering first responders, supervisory and command members, and other relevant stakeholders, with the purpose of providing enhanced public safety while also ensuring overall accountability related to department members and engaged persons.

A. Description and Purpose of the Technology

A - 1. Aircraft Mounted Camera Systems (AMC)

1 The fixed-wing aircraft operates at a significantly higher altitude than the rotary-wing aircraft (helicopter) utilized by the department (fixed-wing aircraft operates at 3000+ ft above ground level (AGL); helicopter operates at 500-700 ft. AGL). The fixed-wing aircraft aims to reduce noise/light pollution as well as work to limit potential trauma incurred by the community members of Oakland who may have a negative association with or reaction to the sound of the department rotary wing aircraft (helicopter).

2 A byproduct of the higher altitude of the fixed-wing aircraft is that a FO can no longer rely on observing, with the unaided eye, through the window of the aircraft to make accurate and beneficial observations as to what is occurring on the ground. The FO must instead rely on a high-definition pan-tilt-zoom camera, specially designed for use at altitude, and mounted onto the body of the aircraft.

3 An aircraft mounted camera system (AMC) will need to be utilized throughout the entirety of the flight (but shall only record as described in Sec. B below) while responding to assist with dispatched calls, critical incidents, search and rescue operations, mitigating vehicle pursuits (allowing ground units to disengage), and a variety of other roles previously conducted by the department's rotary wing aircraft.

A - 2. Downlink System Component

The Downlink component of the system allows the video and pictures captured by the AMC to be streamed via a secure wireless connection to those devices authorized by this policy. Downlink is functional whether the AMC is operating in the passive or active recording modes. Utilizing Downlink offers the opportunity to provide department members, city leaders, and other emergency responders with a greater overall picture of what is occurring during critical incidents. This has the potential to provide valuable information allowing for more informed decisions that enhance the safety of the community and first responders. Downlink has the capability of being utilized during natural disasters (e.g., earthquakes, fires, flooding etc.) to allow emergency personnel to assess evacuation routes, direct responders, and coordinate emergency efforts.

The Downlink component can also be used to ensure more effective command and control and enhanced accountability during critical incidents and crowd control events as defined in Training Bulletin III-G[1]. This technology is authorized to be used during First Amendment activity as defined in the above policy at the direction of the Chief of Police or their designee. The AMC will be under the same restrictions regarding recording in a manner that minimizes interference with people lawfully participating in First Amendment activities. Utilization during crowd control events would aim to reduce the need for officers to be in direct contact with large crowds in the event there are a small number of violent agitators who conceal themselves within a group of peaceful demonstrators, as has been observed during previous crowd control events. Downlink allows commanders a comprehensive overview with which

[1] Any recordings captured during crowd control events shall be taken and managed in accordance with Training Bulletin III – G.

to plan field operations that focus on safely facilitating members of the community being able to demonstrate and exercise their constitutional rights in public spaces. The live feed will allow commanders to coordinate appropriate traffic control to safely facilitate marches, respond to medical emergencies within the crowd, and when necessary, safely plan the apprehension of specific agitators who pose a danger to the community or significant property, while at the same time, limiting the potential impact on the overall group.

Downlink will also play a critical role in responding to unlawful, dangerous, and often violent sideshow activity throughout the City of Oakland. The use of Downlink in these circumstances will facilitate the documentation of dangerous unlawful activities conducted by participants in sideshow events, as well as provide critical information to commanders which will be used in planning the Department's measured response.

A - 3. Aircraft Mounted Camera Modes

The Aircraft Mounted Camera (AMC) has several modes in which it can be operated. These modes can be separated into two major categories:

- Color Camera: Used during daytime operations and provides High-Definition Color video and still images to the Flight Observer (FO) monitoring the images within the aircraft.
- Infrared (IR) Camera: Used to search for heat signatures during low light/visibility conditions. Infrared is an energy similar to visible light, but with a longer wavelength. Infrared energy is invisible to the human eye, however, while visible light energy is emitted by objects only at a very high temperature, infrared energy is emitted by all objects at ordinary temperatures. Since thermal imagers sense infrared energy, which varies with the temperature of objects in a scene, the image generated provides a thermal signature of the scene. This image can be displayed on a standard video monitor.

Infrared energy from objects on a scene are focused by optics onto an infrared detector. The infrared information is then passed to sensor electronics for image processing. The signal processing circuitry translates the infrared detector data into an image that can be viewed on a standard video monitor.

Thermal imaging systems not only make it possible for FO's to make observations in the dark but also enhance the ability of the FO to detect critical objects not visible otherwise. Warmer objects such as people and

animals stand out from typically cooler backgrounds. This allows a FO to provide critical information to ground units, which may prevent surprise chance encounters between officers and an engaged person or an aggressive animal, both of which may be avoided by creating time and distance by way of the Air Unit's observations. Thermal imaging systems are significantly more effective than the unaided eye in daylight, night, and most poor weather conditions. IR cameras *cannot* see through walls, rooftops, or glass. However, IR cameras are capable of seeing through smoke which can be critical in a firefighting or rescue environment.

Either of these modes (Color Camera/IR) can be recorded and stored digitally on a hard drive for later upload and can also be transmitted via Downlink as approved within this policy.

B. Use of the Aircraft Mounted Camera (AMC)

B - 1. AMC Recording Modes (Active/Passive)

Active recording is defined as initiating the visual recording capabilities of the AMC. When the AMC is not actively recording, it is passively recording video in a 30-second continuous moving loop, often referred to as a 30-second rollback. When the AMC recording is activated by the operator, it saves this video-only (no audio) clip of the 30-second period prior to activation and continues recording until stopped by the operator. This technology is functionally similar to the Department's Body Worn Camera (BWC) policy DGO I-15.

Due to the time required for the AMC to initialize and become ready for use the AMC will be turned on while on the ground and can utilized during the entirety of the flight. This will enable the FO to monitor activity on the ground for the duration of the flight. Unlike the rotary wing helicopter, the FO in an airplane does not have the ability to look out the window and effectively observe actions on the ground due to the low wing design of the airplane as well as the altitude that the aircraft will typically be operating at: 2500-4500 feet above ground level (AGL). FO's frequently observe crimes and other incidents such as reckless driving, vehicles fleeing the scene of a violent felony, vehicle collisions, fires, etc., in public areas throughout the city. In many instances, the Air Unit is capable of responding to an incident prior to the arrival of ground units. This allows the Air Unit to provide critical information to units on the ground such as the location and condition of a victim of a shooting, a person injured from a significant collision, or even incidents of a missing person. In other incidents, the Air Unit may be able to advise of the location of a potential suspect related to a violent crime and

information which may allow officers to respond with special consideration for creating time and distance from a potentially armed subject, key elements of de-escalation and preventing violent confrontations between an armed engaged person and officers. Without the ability to effectively observe these incidents, officers cannot relay critical information to dispatch, thereby delaying emergency response.

Once the AMC is placed in the active recording mode, the observations made by the AMC will be recorded continuously until the FO deactivates the recording or the data storage device is full. It should be noted that, unlike the BWC, the AMC does not capture live audio in conjunction with the video recording. The AMC is capable of capturing radio traffic which is synced with the video at the time of the recording.

Each time the camera is turned off or placed in a storage condition the device will experience a delay, up to several minutes, in order to realign itself with the aircraft and recalibrate the onboard sensors. These delays could cause significant information/data to be uncaptured during a critical incident which could adversely influence the outcome of the investigation and those involved. For this reason, while operating the aircraft the AMC shall be maintained in the passive mode or active recording mode while the aircraft is in flight and operating in a potential enforcement capacity.

B - 2. Required Activation of the AMC

Members operating the AMC shall only activate the recording function on the AMC camera in the following circumstances:

1. Members are actively involved in a detention and/or arrest and this information is known to the operator of the AMC;
2. Members are actively conducting a search of a yard, building, area, or vehicle, where a suspect is anticipated to be located or to rule out the presence of a suspect.[2]
3. While members are conducting an assessment or evaluation for a psychiatric detention pursuant to Welfare and Institutions Code § 5150, and where the engaged subject has been observed as actively violent towards community members or officers;

[2] This does not include situations where officers are conducting a perimeter for a prolonged period, where a search is not actively being conducted, and the actions of the suspect are not able to be observed by the Flight Operator.

4. Members on the ground are engaged in a pursuit, as defined in DGO J-04, *Pursuit Driving;*
5. The Air Unit is actively engaged in following a vehicle following the termination of a pursuit or other criminal activity, where enforcement action by ground units is pre-planned or imminent;
6. While members are actively serving a search or arrest warrant and the location has not yet been determined to be secured;
7. When members are observed taking any enforcement action or when the AMC operator is directed to activate the recording feature by a supervisor or commander during a crowd control situation in the City of Oakland (*Training Bulletin III-G*). Activation of the recording function of the AMC during Crowd Control or First Amendment related activities shall only be for the purpose of documenting crimes that are actively occurring, documentation of items that may be of evidentiary value during a subsequent investigation, or any time when an unlawful assembly has been declared in accordance with the California Penal Code Section 407.

B - 3. Deactivation of the AMC

Once activated pursuant to B-2, Members shall not deactivate the AMC recording until one of the following occurs:

1. It is determined by ground units or the AMC operator that there is no person related to criminal activity present at the scene of the incident and anticipation of contact with such persons is unlikely;
2. The Air Unit's involvement in the contact, detention, search, or arrest has concluded;
3. Members have concluded a search of a yard, building, area, or vehicle, and are no longer actively searching for a suspect, or in situations where the Air Unit is no longer involved in a search;
4. The Air Unit terminates its involvement in following a vehicle that was involved in a pursuit or other criminal activity;
5. They receive an order from a higher-ranking member. That higher ranking member shall note the reasoning for deactivation via Computer Aided Dispatch (CAD), their BWC, or report;

If circumstances arise requiring re-activation members shall re-activate pursuant to B-2, above.

A - 2. Prohibited Use

1. AMC shall not be equipped with analytics capable of identifying groups or individuals, including but not limited to Artificial Intelligence, facial recognition, gait analysis, predictive analytics, or Automated License Plate Reader (ALPR).
2. AMC shall not be used for the following activities:
   a. Conducting surveillance of anyone not subject to an active investigation.
   b. Targeting a person or group of people based on their characteristics, such as but not limited to race, ethnicity, national origin, religion, disability, gender, clothing, tattoos, sexual orientation and/or perceived affiliation when not connected to actual information about specific individuals related to criminal investigations.
   c. For the purpose of harassing, intimidating, or discriminating against any individual or group.
   d. To conduct personal business of any type.

A - 3. Discretionary Activation

When not required to activate or prohibited from activation as described above (see B - 2- and B - 3), members may use their discretion when deciding to activate or de-activate the AMC recording functionality if it is in furtherance of an active investigation and serves a legitimate law enforcement purpose. Examples include activations of the recording function to document instances of reckless driving that may not later be documented in a crime report, or documentation of a fire scene that may later be determined to be Arson. At the time of the recording the Flight Observer may not be able to immediately determine if it meets one or more of the above criteria.

A - 4. Privacy Considerations

AMC Operators shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure) without a search warrant unless exigent circumstances exist.

When OPD Aircraft are being flown and the AMC is being utilized, operators should take steps to ensure the camera is focused on the areas that are necessary to the task and to minimize the inadvertent collection of data about uninvolved persons or places. Operators and observers shall take reasonable precautions, such as being conscious and deliberate with the positioning of an imaging device, to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy.

A - 5. AMC Use Documentation

Members are required to document all activations of the AMC recording function, except for tests or accidental recordings. Documentation shall be made in the Aircraft Flight Log (TF-488A). Delayed or non-activations of the AMC, when activation was required by policy, shall be documented in the appropriate report, and reported to the member's supervisor. Such use documentation shall be included in the annual report required by O.M.C. Ch. 9.64, and periodically audited to ensure compliance with this policy.

A - 6. Data Upload

Members shall upload AMC data files (videos) at the conclusion of their shift, or if directed by a supervisor, during their shift, to ensure local storage capacity is not exceeded.

A - 7. Annotation and Categorization of AMC Files

All members shall annotate AMC data files (videos) daily, or, if not feasible, by the end of the member's next regularly scheduled workday. The following information shall be annotated on every AMC data file:

- The report number associated with the incident recorded (in the ID field);
- or the incident number (in the ID field if there is no report number associated with the incident being recorded).
- The category of the video using the appropriate retention category (on Evidence.com).

If neither the report number nor the incident number exists, members may use the letters "NA" or leave the ID field blank. Members are authorized to view their video in order to identify the file for annotation unless otherwise prohibited by policy. During incidents that require exceptional resources or large-scale activation of Department members (e.g. natural disaster), the incident commander may approve delayed annotation of AMC files except in cases that require an investigative call-out. The incident commander shall document any such orders in the appropriate after-action report.

B. AMC Data Management

B - 1. Data Collection

The activation and deactivation of the recording capabilities and subsequent data collection shall be in accordance with sections B - 2 through B - 5 of this policy. The AMC operator will maintain the integrity of a dedicated AMC data storage device and shall not overwrite or delete the video files contained within, until which time the data is uploaded onto the Evidence.com servers.

B - 2. Court and Judicial Proceeding AMC File Copies

1 Personnel requiring a copy of AMC audio/video file(s) for court (e.g., for Traffic court, or a proceeding in a different county) shall contact their first line supervisor or their designated System Administrator (for non-patrol assignments). If the first line supervisor is unavailable, personnel shall contact any System Administrator. Any AMC copies not entered into evidence shall be returned to the first line supervisor or a System Administrator for destruction.

2 CID and other investigative personnel taking a case to the District Attorney (DA) for charging are responsible for obtaining copies of, and/or using the evidence.com secure sharing capability to share, all applicable AMC files for presentation to the DA.

3 Prior to copying the AMC video file, members authorized to make copies shall document the reason for making the copy and the name of the person receiving the copy in the "Notes" field of each video file copied. If applicable, the name entry shall also include the person's rank and serial number.

4 The person receiving the copy shall maintain the copy in a secure location until it is needed for court or custody is transferred to another person.

5 Additionally, they shall document, as soon as practical, the name and/or position of the person receiving the copy in the "Notes" field of each video file.

6 The documentation of the chain of custody and responsibility to secure the copy shall transfer to the person receiving the copy until:

7

- The copy is received by non-Department personnel (e.g. District Attorney, City Attorney, Court Clerk, etc.);
- The copy is admitted into evidence; or
- The copy is returned to a system administrator for destruction.

B - 3. Use of AMC Files for Training

Training staff is authorized to view AMC files regarding incidents which may serve as a learning or teaching tool. An AMC file may be utilized as a training tool for individuals, specific units, or the Department as a whole. A recommendation to utilize an AMC file for such a purpose may come from any source.

A person recommending utilizing an AMC file for training purposes shall submit the recommendation through the chain of command to the Training Section Commander.

The Training Section Commander shall review the recommendation and determine how best to utilize the AMC file considering the identity of the person(s) involved, sensitivity of the incident, and the benefit of utilizing the file versus other means.

Any persons or identifying information observable within the video not relevant to the training shall be redacted or obscured in such a manner as to not identify the uninvolved person.

B - 4. Additional Data Access

Outside of the provisions described in C – 2, AMC image and video data that is recorded and stored within the removable drive or on AXON may be shared only with other law enforcement or prosecutorial agencies only as permitted by law, and subject to the following procedures:

1. The agency makes a written request for the OPD data that includes:
   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The basis of their need for and right to the information.
      i. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation.
2. The request is reviewed by the Chief of Police, Assistant Chief of Police, Deputy Chief/ Deputy Director, Criminal Investigations Division Commander or designee and approved before the request is fulfilled.
3. The approved request is retained on file, and incorporated into the annual report pursuant to Oakland Municipal Code Section 9.64.010 1.B.

B - 5. Data Protection and security

All AMC data storage devices (SD Card, Flash Drive, Portable Hard Drive) will be secured in a manner (e.g. lockbox) only accessible to Air Support Unit (ASU) personnel. All evidence from ASU data devices shall be uploaded to the Evidence.com server and then immediately removed from the drive.

B - 6. Data Retention

In line with the existing DGO I-15- Body Worn Camera (BWC) Policy, which utilizes the same cloud storage platform (Evidence.com) AMC files shall be retained for a period of six months unless it is required for:

1. A criminal investigation;
2. An administrative investigation; (Internal Affairs)
3. Research; (to be approved by the Chief of Police or their designee)
4. Civil litigation;
5. Training; and/or
6. No recordings shall be deleted while any request for the recordings is pending, including but not limited to a public records request or litigation hold request

AMC files that are not flagged for retention for any of the above reasons will be automatically deleted by the File Management System's data retention processes, which are set and maintained by the Project Administrator or designee. This retention process is already in place and utilized for BWC data.

B - 7. Public Access

AMC data which is collected and retained under section C - 6 of this document is considered a "law enforcement investigatory file" pursuant to Government Code § 6254, and shall be exempt from public disclosure. The Department will disclose recordings as appropriate pursuant to statute or court order. AMC data which is retained pursuant to section C - 6 shall be available via public records request pursuant to applicable law regarding Public Records Requests as soon as the criminal or administrative investigations have concluded and/or adjudicated.

C. ADMINISTRATIVE INFORMATION

C - 1. Training

The ASU Unit Supervisor, or other designated OPD personnel, shall ensure that all authorized operators and required observers have completed all department-approved training in the operation, applicable laws, policies and procedures regarding the use of the AMC and downlink. This annual training will be documented utilizing a policy compliance attestation form to be created upon implementation of this policy.

C - 2. Auditing and Oversight

The ASU unit supervisor, or other designated OPD personnel, shall develop a protocol for documenting all AMC uses in accordance with this policy with specific regard to safeguarding the privacy rights of the community and include this in the AMC procedure manual and the annual AMC report. The ASU supervisor will develop an electronic record of deployments and recordings created. The operator of the AMC will document the deployments in the appropriate flight logs. This protocol will allow the ASU supervisor to have a continuous log of all deployments and assist with completing the annual report.

C - 3. Maintenance

The ASU unit supervisor, or other designated OPD personnel, shall develop an AMC inspection, maintenance, and record keeping protocol to ensure the continuing functionality of the AMC, and include this protocol in the AMC procedure manual. Maintenance and record-keeping should also include expenditures such as purchase of new equipment, required updates and mechanical repairs.

C - 4. Description of the Technology AMC File Management System

The AMC system employed by OPD features upload computer stations and an internet web interface for controlling how files are uploaded and archived. The interface allows for Internet Protocol restriction features to control the locations where the system can be accessed. These restrictions limit AMC video file access to only authorized OPD personnel. Videos that are tagged for any reason as part of an investigation are moved to separate folders where they cannot be deleted. The cloud-based archive system has built-in redundancy with multiple servers to ensure data integrity and CJIS compliance.

1

By order of

Darren Allison
Interim Chief of Police Date Signed: _____

L3HARRIS™
FAST. FORWARD.

WESCAM MX™-15.
FULLY DIGITAL. HIGH DEFINITION.

PAYLOAD SPECIFICATIONS	
Sensor Options for Thermal Imager (Select #1a or #1b)	
Sensor #1a - Thermal Imager:	
Type:	MWIR, cooled
Resolution:	640 x 512 Pixels
Fields-of-View:	26.7° to 0.54°
Sensor #1b - HD Thermal Imager:	
Type:	MWIR, cooled
Resolution:	1280 x 1024 Pixels
Fields-of-View:	35.5° to 1.2°
Sensor #2 - HD Daylight Zoom:	
Type:	Color
Resolution:	1920 x 1080 Pixels
Fields-of-View:	31.2° to 1.2° - 720p, 31.2° to 1.8° - 1080p
Sensor Options for Low-Light Continuous Zoom and SWIR Continuous Zoom (Select #3a or #3b)	
Sensor #3a - Low-Light Continuous Zoom:	
Fields-of-View:	40.8° to 2.4°
Sensor #3b - SWIR Imager Continuous Zoom:	
Fields-of-View:	40.8° to 2.4°
Sensor #4 - HD Daylight Spotter:	
Type:	Color
Resolution:	1920 x 1080 Pixels
Fields-of-View:	0.72° to 0.29° - 720p, 1.1° to 0.43° - 1080p
Sensor Options for MX-Day/Night Spotter (Select #5a or #5b)	
Sensor #5a - HD Low-Light Spotter: (Used with Sensor #4)	
Resolution:	1920 x 1080 Pixels
Fields-of-View:	0.72° to 0.29° - 720p, 1.1° to 0.43° - 1080p
Sensor #5b - HD SWIR Spotter: (Used with Sensor #4)	
Sensor #6 - Laser Illuminator (LI)[1]:	
Wavelength:	860nm (near IR)
Beam Power:	700mW
Beam Divergence:	Wide, Narrow or Ultra Narrow
Sensor #7 - Secondary Laser Illuminator (LI)[1]:	
Wavelength:	860nm (near IR)
Beam Power:	150mW
Beam Divergence:	Narrow
Sensor #8 - Laser Rangefinder[2]	
Wavelength:	1.54µm
Range:	20km
Additional WESCAM MX-15 Features and Embedded Options:	
> Optical Bench IMU > AutoTracker > GPS Receiver	> Moving Target Indicator > LDDT (SWIR tracking of multiple 3rd party designator spots)
Notes:	All FOVs are for digital outputs: Consult factory for FOVs for analog outputs up to 4x Ezoom available.

TURRET SPECIFICATIONS	
Stabilization and Steering	(4) Axis + (6) DoF Isolator Azimuth Range: Continuous 360° Elevation Range: +90° to -120°

SYSTEM SPECIFICATIONS	
WESCAM MX-15 Turret	<95 lbs / 43.2 Kg (all sensors), 15.5”(D) x 18.95”(H), 393.7mm (D) x 481.33mm (H)
Power	MIL-STD-704F, 280W (Avg.)

FEATURES AND BENEFITS

> Multi-Sensor Imaging/Lasing Payload Options

> Short-Wave Infrared (SWIR) Imaging

> High-Performance Gimbal

> Advanced Image Processing

> Interface Flexibility

> Ruggedness

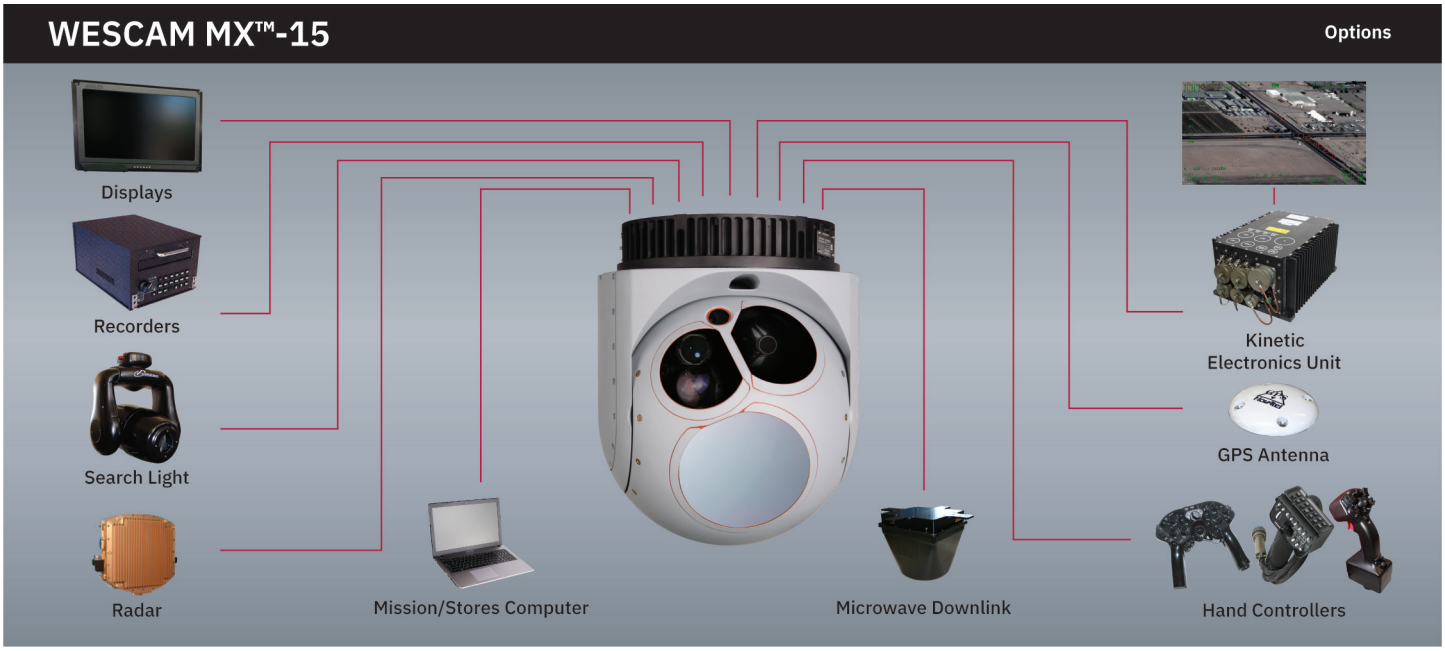
> Simplified Aircraft Integration

The WESCAM MX-15 is an advanced, industry-leading stabilized multi-sensor, multi-spectral imaging system that is renowned for high performance, operator ease-of-use, and reliability. It's ideal for a wide range of missions, including medium altitude covert intelligence, surveillance, and reconnaissance, armed reconnaissance, search and rescue. The system provides imagers for optimal performance in a wide range of conditions; bright sunlight, overcast/dusk, smoke, and complete darkness. That is supported by a suite of advanced image processing algorithms for noise reduction, sharpening, and local area contrast enhancement that aid feature recognition.

Superior stabilization is the key to achieving the maximum target detection, recognition, and identification range performance from the imagers. The WESCAM MX-15 achieves this with a hybrid active and passive jitter suppression system. This proven architecture stabilizes all devices on the optical bench equally. In addition, stable and accurate target geolocation ensures that the crosshairs stay on a stationary target, regardless of changes to aircraft position, attitude, and heading. This significantly reduces the operator burden in keeping eyes on target.

Advanced processing features such as object tracking, image blending, and moving target indication further serve to automate the search and tracking process, allowing the operator to focus on the target versus the equipment.

To ensure that the WESCAM MX-15 is fit for the mission, it is fully qualified to MIL-STD-810 for environmental withstanding, MILSTD-461 for electromagnetic compatibility, and MIL-STD-704 for power quality.



VIDEO INTERFACES
Built-in video switch matrix
6 independent HD-SDI output channels available
5 analog video (NTSC or PAL) output channels available

DATA INTERFACES
Interface Types: RS-232/422, Ethernet, MIL-STD-1553B, ARINC 429
Functional Interfaces: Aircraft GPS/INS, Remote Control, Moving Map, Microwave / Data Link, Searchlight, Radar, Metadata / Status
HMI Options: Moving Map, Mission Console
Compatible with WESCAM Microwave Communications Equipment.

WESCAM MX-15

© 2021 L3Harris Technologies, Inc. | MX15-0503AA-Spec

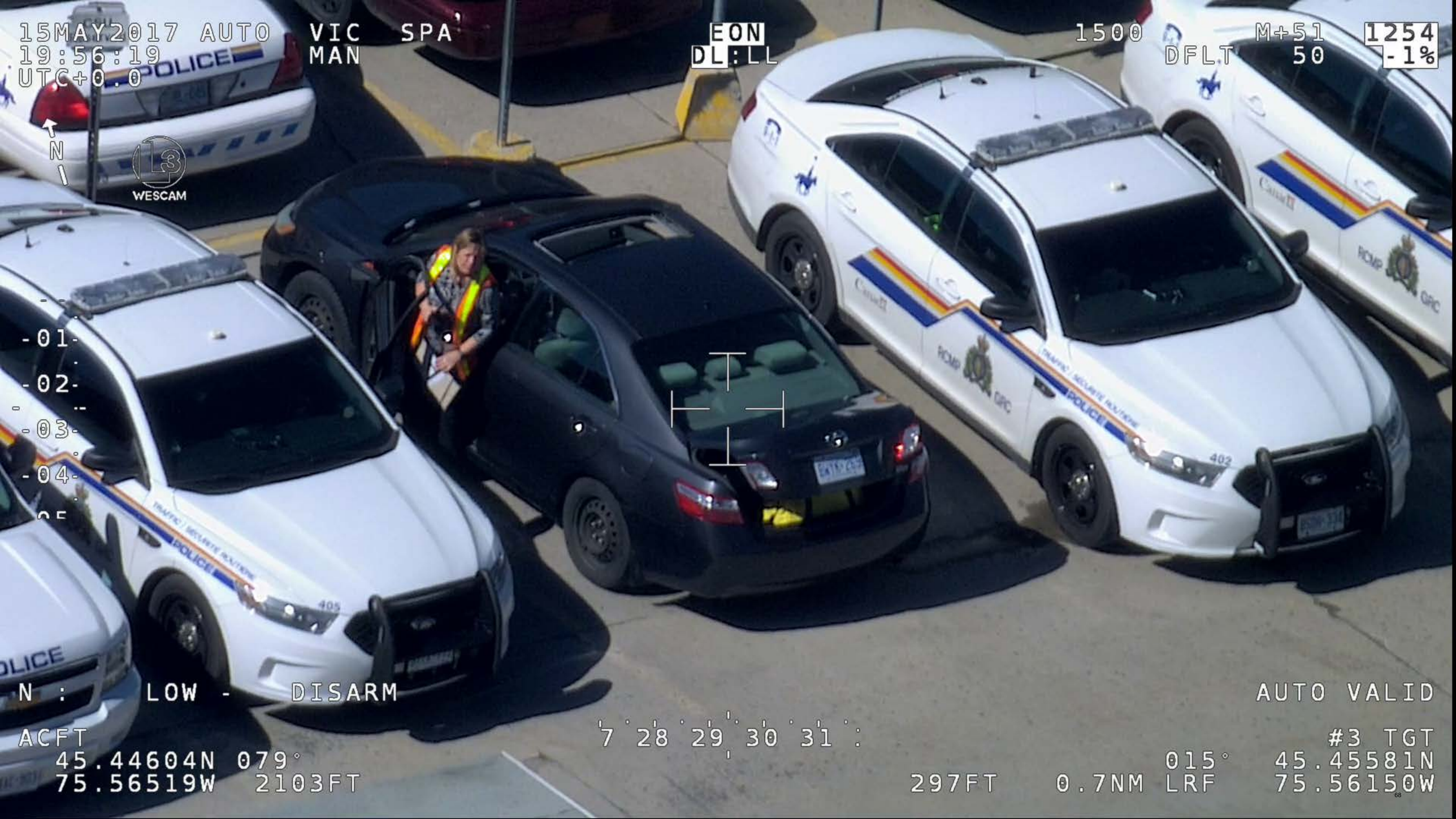
[1] [2] Consult factory for specific environmental and target conditions

L3HARRIS™
FAST. FORWARD.

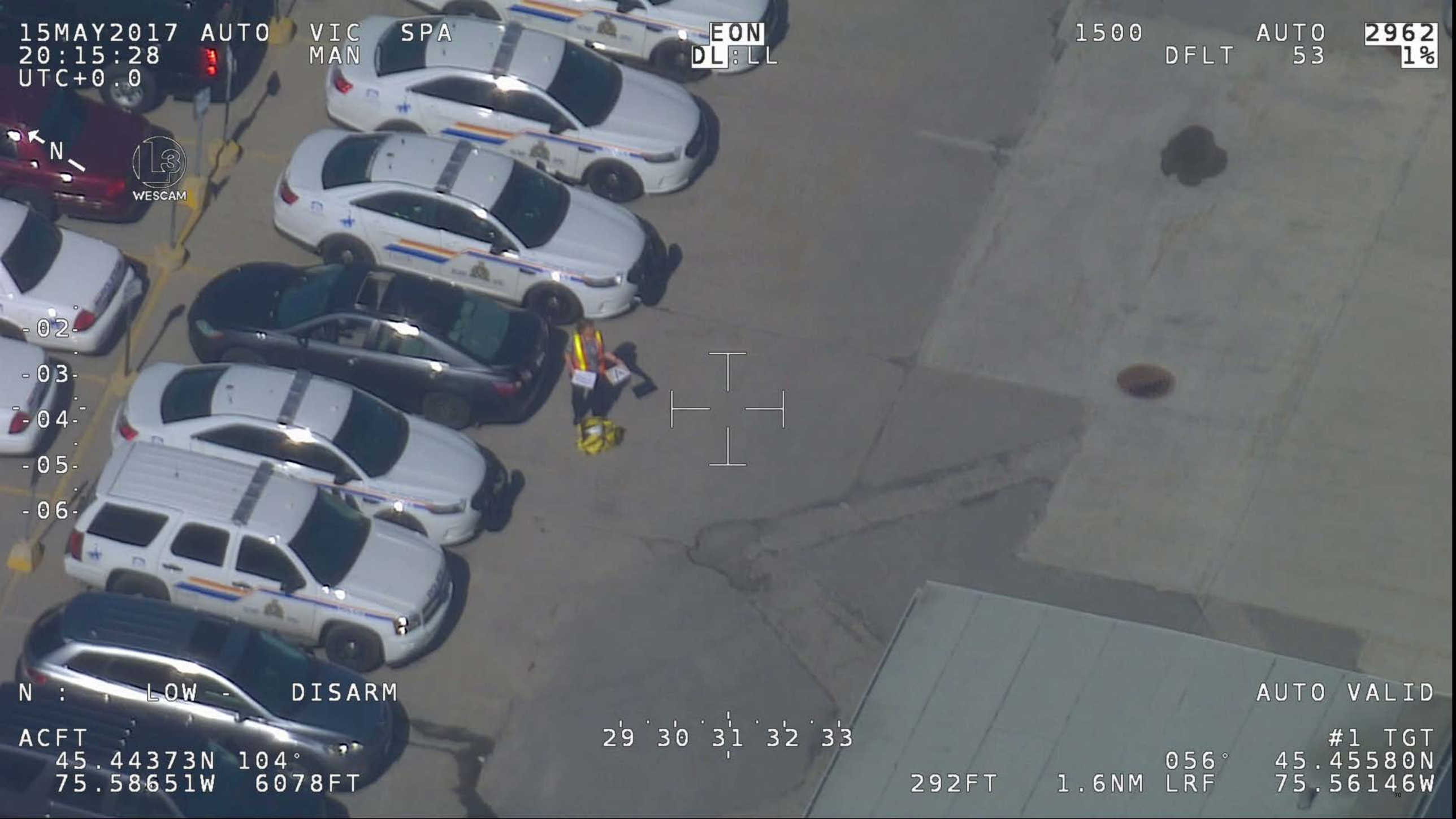
1025 W. NASA Boulevard
Melbourne, FL 32919
t 1 800 668 4355
info.wescam@L3Harris.com

The information contained within this product data sheet is not subject to export controls and may be released without export restrictions. The equipment described herein may require Canadian and/or U.S. Government authorization for export purposes. Diversion contrary to Canadian and/or U.S. law is prohibited.

27NOV2018 AAID VIC SPA
17:19:56 MAN
UTC-7.0
IR BH
587
AUTO 1563
DFLT AUTO 0%
MX15HDI
1677
N
WESCAM
-020°
260°
OFF NONE
ACFT
40.52815N 348°
104.97215W 6619FT
NEWPOI TGT
251° 40.52394N
4846FT 1565M LOS 104.98858W


15MAY2017 AUTO VIC SPA
19:56:19 MAN
UTC+0.0
EON
DL:LL
1500
M+51
DFLT 50
1254
-1%
N
WESCAM
-01-
-02-
-03-
-04-
N : LOW - DISARM
AUTO VALID
ACFT
7 28 29 30 31
#3 TGT
45.44604N 079°
75.56519W 2103FT
297FT
015° 0.7NM LRF
45.45581N
75.56150W

15MAY2017 AUTO VIC SPA
20:07:18 MAN
UTC+0.0
IR
880 AUTO
DFLT AUTO
2842
-9%
N
WESCAM
-01-
-02-
-03-
-04-
-05-
N : LOW - DISARM
AUTO VALID
ACFT
45.46444N 255°
75.54540W 5977FT
3 24 25 26 27
#1 TGT
147° 45.44732N
303FT 1.5NM LRF 75.52990W


15MAY2017 AUTO VIC SPA
20:15:28 MAN
UTC+0.0
EON
DL:LL
1500 AUTO 2962
DFLT 53 1%
N
WESCAM
-02-
-03-
-04-
-05-
-06-
N : LOW - DISARM
AUTO VALID
ACFT
45.44373N 104°
75.58651W 6078FT
29 30 31 32 33
#1 TGT
056° 45.45580N
292FT 1.6NM LRF 75.56146W

27NOV2018
14:02:39
UTC-7.0
AUTO
VIC
MAN
SPA
EON
DL:SW
1500
AUTO
DFLT
50
MX15HDI
1677
N
WESCAM
-027°
332°
AUTO VALID
ACFT
40.53488N 249°
104.97438W 10585FT
226°
4917FT
4396M
LRF
NEWPOI TGT
40.51206N
105.00435W

27NOV2018 AUTO VIC SPA
13:50:49 MAN
UTC-7.0
IR BH
880 AUTO 1391
DFLT AUTO
MX15HDI
1677
N
WESCAM
-011°
285°
OFF NONE
ACFT
40.53581N 314°
104.96659W 6621FT
NEWPOI TGT
240° 40.52534N
4848FT 2399M LOS 104.99051W

27NOV2018 AAID VIC SPA
14:05:29 MAN
UTC-7.0
EON
DL:SW
1500 AUTO
DFLT 50
MX15HDI
1677
N
WESCAM
-021°
265°
AUTO VALID
ACFT
40.45417N 111°
104.96503W 10652FT
4783FT 3350M LRF
019° NEWPOI TGT
40.47933N
104.95681W

Oakland Police Department

Airborne Surveillance Video Downlink Solution

Vislink is proposing to provide the Oakland Police Department with a state-of-the-art airborne surveillance video downlink transmit & receive solution that will provide real-time, high quality high-definition airborne images from two aircraft, operating simultaneously, to both fixed and mobile ground receive units.

This high-quality encrypted/secure video downlink solution will provide real-time actionable video images to both command staff and remote users, allowing for critical decision making, enhancement of officer safety and better allocation of resources.

AIRCRAFT TRANSMIT SOLUTION

Vislink is proposing to provide a new AeroLink 6.5 GHz, high power, high definition, RF transmitter in the proposed Diamond DA62 aircraft platform. The Vislink AeroLink RF transmitter can provide up to 4K UHD encoding.

Vislink is proposing a low-cost and no maintenance omnidirectional antenna system for this aircraft, this antenna will be belly mounted. Utilizing a low-cost omnidirectional antenna allows the aircraft to transmit simultaneously to future multiple fixed receive sites, providing greater area coverage

and signal reliability, as well as to mobile command vehicles and hand-held tactical receive systems.

The Vislink RF transmit system will be fully controlled by the aircrafts mapping & navigation system, allowing for easier control by the Tactical Flight Officer.

FIXED RECEIVE & DISTRIBUTION SOLUTION

Vislink is proposing to provide and install a single 2-channel fixed receive site solution on the existing self-support tower structure or building structure within the City of Oakland. The proposed Vislink solution will allow any two aircraft to simultaneously transmit live video downlink images, into the fixed receive system.

The proposed fixed tower solution receives the aircraft signals and then provides an IP output stream, which is then transported over the cities secure data network to the Police EOC facility, where the actionable video images it can be viewed by command staff on a video wall or dedicated television monitor.

Additionally, Vislink will provide a secure cloud distribution and viewing system, no video recording or storage will be provided. The downlink images will be sent to an AWS Government Cloud instance, where the video can be observed by only authorized users, via password protection.

This solution allows for a hands-off viewer approach, allowing command staff access to actionable video images, without he need to initiate the downlink reception from the command center.

PORTABLE / TACTICAL HAND-HELD RECEIVE SOLUTION

Vislink will also provide one of our MobilCMDR portable / tactical hand-held receive kits. This self-contained hand-held receiver allows for direct viewing of encrypted aircraft video downlink images on a daylight viewable screen, as well as connection to an external monitor via a coax cable connection.

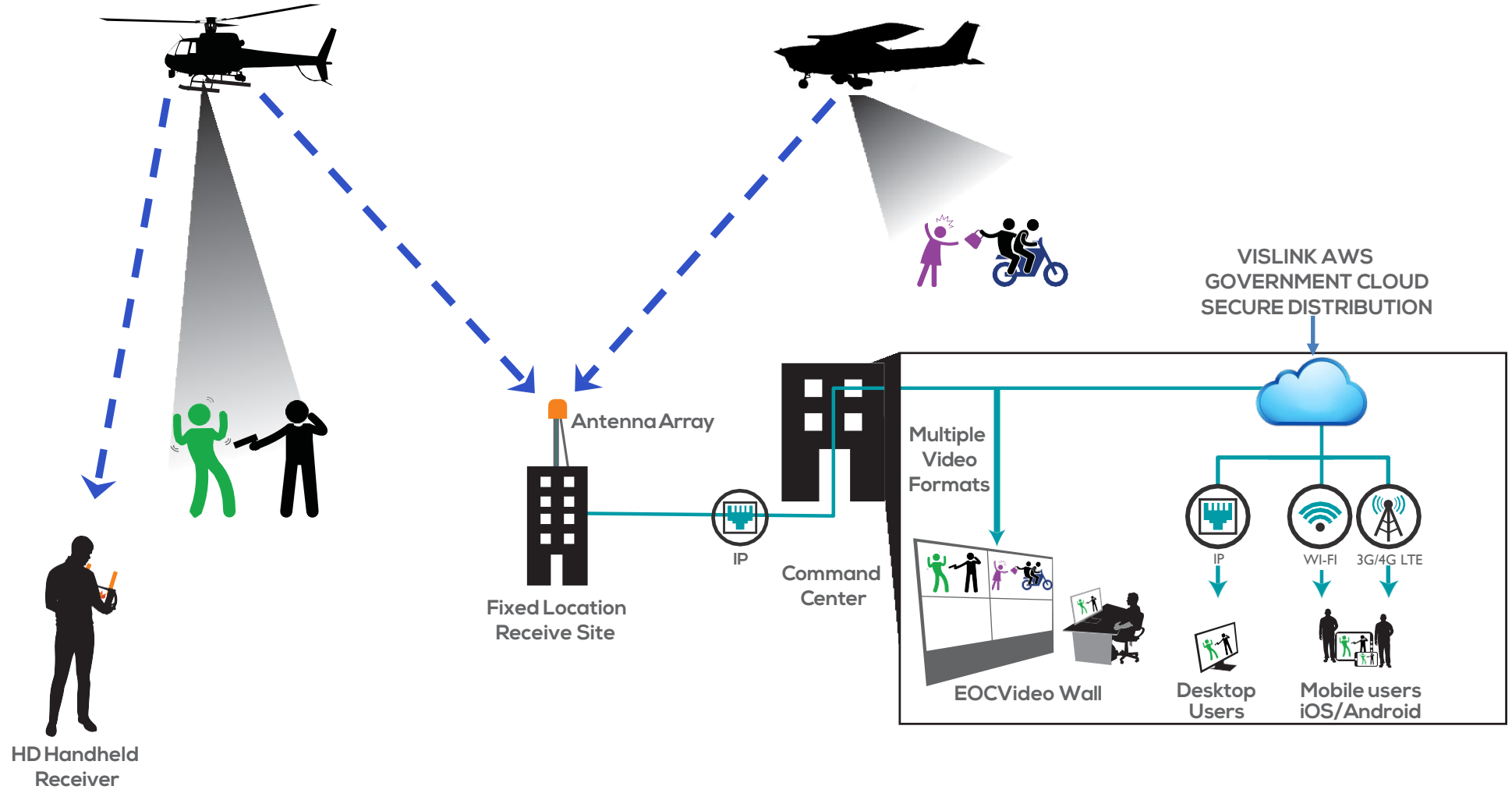
This unit can also be utilized at the police aviation hangar to test the aircraft transmit system, to ensure proper operation prior to flight.

VISLINK

Oakland Police Department

Airborne Surveillance Video Downlink

Fixed and Handheld Receive Solution



Oakland Police Department

Surveillance Impact Report:
Aircraft Mounted Camera (AMC)/Downlink

---

1. Information describing the Aircraft Mounted Camera/downlink technology and how it works.

Wescam MX-15

The WESCAM MX-15 does not contain any software, technology, or programs that use Facial Recognition, gait analysis, or Automated License Plate Reader (ALPR) technology.

The WESCAM MX-15 is an advanced, industry-leading stabilized multi-sensor, multi-spectral imaging system that is renowned for high performance, operator ease-of-use, and reliability. It is ideal for a wide range of objectives, including, Emergency Services, airborne law enforcement, and search and rescue. The system provides cameras for optimal performance in a wide range of conditions such as bright sunlight, overcast/dusk, smoke, and complete darkness. The platform is supported by a suite of advanced image processing algorithms for noise reduction, sharpening, and local area contrast enhancement that aid in object recognition (Object recognition is the ability to detect people, vehicles or objects in relation to their surroundings (i.e., how well you can see something). Superior stabilization is the key to achieving the maximum object detection, recognition, and identification range performance from the cameras.

The WESCAM MX-15 aircraft mounted camera (AMC) comes equipped with technology that allows for easy image tracking and stabilization, regardless of what the aircraft is doing, this allows the officer to focus on what is happening on the other side of the camera, instead of worrying about how to effectively use the camera.

VISLINK DOWNLINK

The Vislink Downlink System will provide the Oakland Police Department with a state-of-the-art airborne video downlink transmit & receive solution that will provide real-time, high quality high-definition airborne images from the aircraft, operating simultaneously, to both fixed and mobile ground receive locations.

This high-quality encrypted/secure video downlink solution will provide real-time actionable video images to both command staff and remote users, allowing for critical decision making, enhancement of officer safety and better allocation of resources.

2. Proposed Purpose

At the direction of the Oakland City Council, Oakland Public Safety Committee, Reimagining Public Safety Task Force and the Oakland Police Department, the Air Support Unit has explored numerous alternatives to the current methods and equipment utilized by the Air Unit. After careful consideration to include, product testing/evaluation, fiscal analysis, stakeholder input, and industry standards, the Department has requested that a fixed wing aircraft be purchased for use by the Air Support Unit. The proposed camera technology which will be installed on the aircraft will allow the Flight Observer (FO) to observe in real time what is occurring on the ground prior to ground units arriving on scene. The fixed wing aircraft which will fly at a much higher altitude than the current aircraft, (3000+ ft above ground level (AGL) vs. 500-700 ft. AGL that the helicopters fly at). This will immediately reduce noise/light pollution as well as the emotional trauma incurred by the citizens of Oakland who have a negative association with the OPD helicopters. A byproduct of this higher altitude is that FO's can no longer look out the window to observe what is occurring below and must rely on a high-definition camera to make their observations. This Camera and any subsequently purchased aircraft mounted cameras will need to be utilized throughout the entirety of the flight while responding to dispatched calls as well as to proactively be on the lookout for criminal activity much as an officer would look out their vehicle window while on routine patrol. Aircraft mounted cameras have existed on the OPD helicopters for over two decades. This technology however is outdated and ineffective to perform the tasks that the Air Support Unit is currently tasked with. While the camera will be utilized throughout the entirety of the flight the recording capabilities will only be employed under the circumstances specified below and the data that is to be recorded and stored will be required to meet the associated requirements.

The downlink component of the system allows the video and pictures captured by the AMC to be streamed via a secure wireless connection to those devices authorized and approved by the department. Utilizing downlink will provide Commanders, Officers, City Leaders and other Emergency Responders a greater overall picture of what is occurring. Downlink can be utilized during natural disasters, earthquakes, fires, flooding etc.) to allow Emergency personnel to assess evacuation routes, direct responders, and coordinate emergency efforts. The downlink can also be used to ensure the efficiency and accountability of officers on the ground. Additional uses of the downlink include utilization during protests to reduce the need of officers being in direct contact with suspects concealing themselves within the crowd, report on direction of travel, and create greater standoff distance with those peacefully protesting. Downlink may also improve situational awareness of unlawful sideshows. This increased situational awareness can be used to assist in de-escalation efforts of various critical instances.

3. Location:

OPD aircraft equipped with the WESCAM MX-15 and VISLINK downlink system may be deployed within the city of Oakland in accordance with the Air Support Unit Deployment Plan as directed by the Chief of Police or their designees. The OPD helicopters and airplane serve as a patrol unit in the sky and may respond anywhere within the jurisdiction of the Oakland Police

Department. The OPD Air Support Unit is occasionally requested to assist with investigations in neighboring jurisdictions and would respond as available to assist with those in accordance with mutual-aid policies and MOU's currently in place. All policies for the use of the associated equipment would be in effect as stated in the Aircraft Mounted Camera Use Policy.

4. Impact:

The AMC that is currently proposed is able to obtain high definition images that can be used to identify individuals, vehicles or other information that may not be visible to the naked eye at the altitudes the aircraft will be operated within. Additionally because the aircraft is able to see from an overhead view, it does allow the camera operator to view into areas not commonly visible to the public (back yards, between buildings, terrain etc.) These images provide information that may not be available without these technologies. The mitigations discussed in section 5 below as well as the AMC Use Policy (I-29) identify when the camera may be intentionally utilized to obtain a specific image and also directs users to not intentionally record or transmit non pertinent information. All use of the camera falls under the AMC use policy which expressly prohibits use of the camera in a discriminatory or biased manner. See section 5 and the AMC Use Policy. The Baltimore Police Department was subject to litigation in 2020 related to a contract with an airborne surveillance company which obtained data that was later determined to be in violation of the plaintiffs 4th amendment rights. The analytical software employed by that agency is not being utilized by the department and would be subject to approval by the City of Oakland Privacy Advisory Committee. The Courts further addressed the "injury" that occurred to the complainants by the persistent surveillance utilized by the agency. The data obtained by the particular contractor in this case was indiscriminately obtained, utilized recording constantly and images captured were of the entire city for an extended period of time. All of the data obtained was retained for a period 45 days and often longer without cause. This type of data collection is not utilized by the department and would not fall under the associated policies.

5. Mitigations:

Random audits will be conducted by the department at their discretion to ensure that members are in compliance with the AMC use policy (DGO I-29). The ASU Supervisor will also be responsible for ensuring that each member authorized to operate the AMC and downlink equipment has been properly trained in the authorized and prohibited uses of such equipment. Training shall be documented with the appropriate records and forms as designated by the department.

AMC Operators shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g. residence, enclosed yard, enclosure) unless actively searching for a victim, suspect, or evidence related to a crime etc. When OPD Aircraft are being flown and the AMC is being utilized, operators will take steps to ensure the camera is focused on the areas necessary to the task and to minimize the inadvertent collection of data about uninvolved persons or places. Operators and observers shall take reasonable

precautions, such as turning imaging devices away, to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy.

Retention periods are specified within the AMC use policy and largely follow that of the department's current Body Worn Camera (BWC) retention policy which is largely governed by legal requirements for evidentiary retention. Notable exceptions are the deletion of videos not meeting evidentiary standards or other documented reasons for retention will be deleted after a 6 month period. All video stored within the Axon data storage platform will be held to the same restrictions as BWC video and the viewing of such files will be under the same restrictions as the BWC policy Departmental General Order DGO (I-15.1).

The fixed wing aircraft is further restricted in its use and locations to be flown by Federal Aviation Regulations (FAR) part 91.991 which states

"Except when necessary for takeoff or landing, no person may operate an aircraft below the following altitudes:

(a) ***Anywhere.*** An altitude allowing, if a power unit fails, an emergency landing without undue hazard to persons or property on the surface.

(b) ***Over congested areas.*** Over any congested area of a city, town, or settlement, or over any open air assembly of persons, an altitude of 1,000 feet above the highest obstacle within a horizontal radius of 2,000 feet of the aircraft.

(c) ***Over other than congested areas.*** An altitude of 500 feet above the surface, except over open water or sparsely populated areas. In those cases, the aircraft may not be operated closer than 500 feet to any person, vessel, vehicle, or structure."

These altitude restrictions will ensure that the aircraft is flying a safe distance above the ground and they will also increase the distance from the camera to the ground, thereby decreasing the level of detail in photos that members of the public may believe to be infringing upon privacy interests.

Although the camera will be turned on during low level flight at takeoff and landing there are very few instances when any recording or observations will actually take place. Due to the departure procedures in effect at the Oakland International Airport where the aircraft will be based, the airplane will often be at over 1000 feet above ground level prior to flying over the city of Oakland. Additionally, due to the angle observed by the camera at lower altitudes it is ineffective for the camera operator to utilize the camera at these low altitudes due to terrain, buildings and other obscuration.

6. Data Types and Sources:

The AMC will record using industry standard file types: JPEG, mov, mp4, wav, or RAW. Such files may contain standard color photographs, standard color video, or other imaging technology, such as thermal. The AMC does not record or transmit audio in any way.

7. Data Security:

All AMC data storage devices (SD Card, Flash Drive, Portable Hard Drive) will be secured in a manner (e.g. lockbox) only accessible to Air Support Unit (ASU) personnel. All evidence from ASU data devices shall be uploaded to the EVIDENCE.COM server and then immediately removed from the drive. See Attachment 4 for OPD Data Retention Policy Time Frames

8. Fiscal Cost:

The Wescam MX-15 camera and the Vislink Downlink equipment was included in a RFQ for the aircraft and mission equipment. See Oakland City RFQ ****.

MX-15- $724,881.00

Vislink Downlink system – $265,000.00

There will be no costs associated with training the operators of the AMC as training documents are provided at no cost to the Department. All other training is conducted in house at no cost. Maintenance costs are minimal to include cleaning and cable replacement cannot be determined ahead of time. Routine software updates are included in the cost of the camera.

The purchase of the aircraft will be funded within the departmental budget as allocated by the city council, or with a Loan taken on by the city/department for the purchase of the airplane and associated equipment.

9. Third Party Dependence:

All data collected by the technology to include video recording will be stored in the EVIDENCE.COM server (currently utilized for all BWC data storage). This is not anticipated to increase the cost or decrease the effectiveness of the city's current data storage capabilities.

10. Alternatives:

The Aircraft Mounted Camera SUP (***Attachment A),*** Section 1, "Alternatives Considered", explains that "OPD could continue the status quo of utilizing the OPD Helicopter with the FLIR 8500 Series camera as well as gyro stabilized binoculars to monitor activities occurring on the ground. Continuing in this manner will require the air asset to fly at an altitude considerably lower causing increased sound/light pollution and trauma associated with the helicopter to the citizens of Oakland.

The Alternatives section also considers drone usage. While drones play an integral part in the protection of Oakland residents and visitors, they are limited in their capabilities. The current flight time for drones is approximately 25-30 minutes and speeds of 25 mph. Drones are limited to line of sight and cannot operate in an area greater than 2-3 blocks. Drones are currently not capable of assisting during vehicle pursuits that exceed these speeds or distances as stated above. Due to the busy airspace surrounding the Oakland International Airport, UAV's are extremely limited to the locations, altitudes and ranges that they can fly. UAV's are also limited in their deployment availability. Drones require approval prior to each deployment. Once approval is obtained, the operator must acquire the equipment, respond to the scene, wait for approval from the FAA and then launch the drone. By this time an incident has likely evolved greatly and may have already concluded prior to the utilization of the drone. OPD aircraft typically fly for 1-2 hours and with the purchase of a fixed wing aircraft will have greater flight capabilities with response times frequently of under 1 minute from dispatch to scene arrival.

OPD does have access to outside agency air assets equipped with cameras such as CHP and ACSO. However, OPD must request those agencies to respond for each incident. This creates a significant delay in response times as each of those agencies are located outside of the city of Oakland (CHP operates from the Napa County Airport 30 NM away and ACSO 19 NM). This process can take a significant amount of time which could negatively impact the outcome of a critical incident. Additionally, these neighboring agencies are responsible for large areas of land outside of Oakland (CHP Golden Gate Division covers nearly 7,000 sq miles and ACSO 739 sq. miles). Due to the unique weather patterns experienced by the City of Oakland, weather frequently prohibits neighboring agencies from responding to the city of Oakland for assistance. OPD can better respond to dangerous situations by equipping our own aircraft with cameras capable of the same level of service provided by neighboring agency aircraft and responding in a timely manner.

11. Track Record:

During previous critical incidents the Oakland Police Department has relied on outside agencies to include the California Highway Patrol, Alameda County Sheriff's Office, and Contra Costa Sheriff's office to provide recordings of critical incidents that have involved officers of the Oakland Police Department.

During the George Floyd Demonstrations in 2020, CHP was again requested to provide assistance to the City of Oakland. CHP in addition to the Oakland Air Support Unit provided updates to command and city leaders on the ground. CHP however was able to provide real

time video from overhead to the Emergency Operations Center with City officials such as the Mayor, City Administrator, Police, Fire and Emergency Services Personnel. This Downlink technology was specifically requested by city leaders for events such as this and has been used successfully on many occasions.

In 2020, Contra Costa Sheriff's office captured an Officer involved shooting involving Richmond and Oakland Police Officers. CCCSO was overhead and recording when an armed murder suspect intentionally rammed several Oakland police vehicles in the city of Richmond. The entire shooting was captured by the Sheriff's helicopter and the video was used by the respective investigative bodies after the incident.

In November 2021, Oakland Officers were fired upon by a carjacking suspect. The vehicle was tracked for an extended time by ground and air resources. While attempting to detain the subject, CHP air was overhead recording with their aircraft mounted camera. Video showed the subject ramming multiple patrol cars and later engaging several officers. This incident led to an officer involved shooting that was captured by both BWC and the aircrafts camera. This video was critical to the subsequent investigations by the Criminal Investigations Division, Internal Affairs as well as the Community Police Review Agency.

Attachments

1 AMC/Downlink Surveillance Use Policy
2 Wescam Documents/Images
3 Downlink Documents

L3HARRIS™
FAST. FORWARD.

WESCAM MX™-15.
FULLY DIGITAL. HIGH DEFINITION.

A Multi-Sensor, Multi-Spectral Imaging System in a Single Line Replaceable Unit (LRU)

ACTIONABLE INTELLIGENCE

The WESCAM MX-15 is ideal for medium-altitude, covert ISR, SAR missions and homeland security.

MULTI-SENSOR IMAGING/LASING PAYLOAD OPTIONS

- Supports seven payload items simultaneously
- HD thermal, HD daylight and HD low-light and HD SWIR cameras provide 24/7 imaging
- Continuous wide-angle zoom
- High-magnification step-zoom spotter
- High-sensitivity color low-light imaging
- Eye-safe laser rangefinder[1]
- Laser illuminator[2] in choice of wide, narrow or ultra narrow divergence

HIGH-PERFORMANCE GIMBAL

- 4-axis stabilized turret with internal passive isolator for excellent stabilization performance
- Sharp optics and superior stabilization performance results in industry leading target detection, recognition and identification range performance in the 15” class
- Inertial Measurement Unit (IMU) mounted to optical bench for high target location accuracy
- Inertial Navigation System (INS) auto-align to aircraft

ADVANCED IMAGE PROCESSING

- Real-time image enhancement on all sensors
  - High-performance haze penetration
  - Improved feature recognition and ID
  - 2x, 4x Ezoom
  - Advanced video tracker
  - Imaging blending
  - Embedded Moving Target Indication
  - Pseudo-color IR

WESCAM ADVANCED VIDEO ENGINE (WAVE)

- A high-performing embedded computing engine engineered to support advanced image-processing capabilities
- WAVE architecture includes a state-of-the-art graphics processing unit (GPU) - enabling future advancements in image processing & surveillance automation

INTERFACE FLEXIBILITY

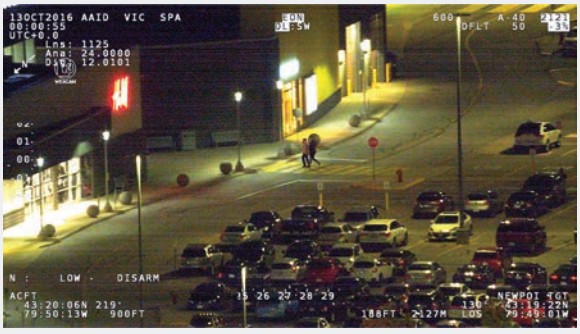
- Built-in video switch matrix provides multiple HD-SDI and analog video outputs
- 720p or 1080p HD video
- Wide range of data ports: RS-232/422, Ethernet, MIL-STD-1553B, ARINC429
- All standard WESCAM MX-Series functional interfaces

RUGGEDNESS

- Rugged aerospace grade aluminum structure
- MilSpec environmental, EMC, and power quality qualification
- Built-in vibration isolator protects internal payload components
- Rigorous environmental stress screening (ESS)
- Designed to minimize maintenance requirements and simplify repair

SIMPLIFIED AIRCRAFT INTEGRATION

- Electronics unit inside the turret
- Built-in vibration isolation
- Built-in GPS receiver
- <19” turret height for better ground clearance
- Compatible with standard quick disconnect mounts
- Side mounted connectors for recessed installations
- No calibration required for LRU swapout



WESCAM MX-15

© 2019 L3Harris Technologies, Inc. | MX15-0501AB-Brochure

[1]Consult factory for specific environmental and target conditions

[2]

L3HARRIS™
FAST. FORWARD.

1025 W. NASA Boulevard
Melbourne, FL 32919
t 1 800 668 4355
info.wescam@L3Harris.com

The information contained within this product data sheet is not subject to export controls and may be released without export restrictions. The equipment described herein may require Canadian and/or U.S. Government authorization for export purposes. Diversion contrary to Canadian and/or U.S. law is prohibited.