CITY OF OAKLAND

Privacy Advisory Commission

December 5, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Regular Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, **Mayoral Representative**: Heather Patterson*

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. Open Forum/Public Comment

3. Review and approval of the draft November meeting minutes

4. Surveillance Equipment Ordinance – OFD – Data Collection for Wildfire District and Fire Safety Inspections Impact Statement and proposed Use Policy – review and take possible action

5. Federal Task Force Transparency Ordinance – OPD – FBI's Joint Terrorism Task Force MOU – review and take possible action

6. Surveillance Equipment Ordinance – OPD – Mobile ID Reader Impact Report and proposed Use Policy – review and take possible action

7. Election of PAC Vice Chair

8. Adjournment at 7:00pm

CITY OF OAKLAND

Privacy Advisory Commission

November 7, 2019 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 M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, **Mayoral Representative**: Heather Patterson*

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

Quorum was reached with these members present: Suleiman, Hofer, Katz, Jacquez, Oliver, and Gage.

2. Open Forum/Public Comment

There were no Open Forum Speakers.

3. Review and approval of the draft October 3 meeting minutes

The October Minutes were approved unanimously.

4. Surveillance Equipment Ordinance – OPD – Live Stream Camera Impact Report and proposed Use Policy – review and take possible action

Captain Randy Wingate presented OPD's revised Use Policies with specific emphasis on the standard that the cameras will only be used during a partial or full activation of the EOC and only with command level approval.

Members Reem, Gage, and Katz who were part of the ad hoc working group also added/ask for clarification on a few items; that specifics be added to the policy describing when an activation occurs,

that language be included regarding any data stored on the cameras themselves. Chairperson Hofer asked for tighter language on uses and on data access—clarifying reasons for law enforcement access.

Captain Wingate will return with a new draft in December.

5. Surveillance Equipment Ordinance – OFD – Data Collection for Wildfire District and Fire Safety Inspections – review and take possible action

OFD Captain Saunders who oversaw the development of the new Wildfire District and Fire Safety Inspections system for the department presented the Impact Statement and Use Policy and provided a demonstration of exactly how the technology works. He explained that the first application was during the wildfire district safety inspections (which inspect the outside of properties) but that the department will be using the same technology to perform commercial building inspections in the future. He explained the need to capture images to monitor inspection quality for auditing purposes, to help identify violations so owners can correct them successfully.

Member Oliver asked what authority OFD has to enter or photograph private areas of a property and other members also asked about the authority to enter and photograph the inside of businesses. Captain Sanders noted the State Fire Code provides this authority and could provide the code number and text for the PAC.
Member gage also asked about training protocols for photographing sensitive areas and Captain Sanders explained the staff are trained to only photograph vegetation during wildfire inspections.

Chairperson Hofer expressed concern about merging the two types of inspections into one Use Policy due to past experience with other technologies that have different uses and suggested separating them may be appropriate. Ultimately the PAC agreed to keep them together but to delineate the difference in the policy.

There was one public speaker: Ken Pratt raised concerns about OFD or their agents being in people's private tards for inspection purposes.

OFD will return in December with a revised policy.

6. Federal Task Force Transparency Ordinance – OPD – FBI's Joint Terrorism Task Force MOU – review and take possible action

Chairperson Hofer first allowed the public speakers on this item to speak.

Javeria Jamil, Mohamed Talib, and Jeffrey Wang al spoke about the concerns they have with how the FBI has conducted itself in regard to JTTF investigations in the past. Thy cited a recently published White paper that highlighted questionable practices. At issue for the policy discussion is whether OPD officers involved in the JTTF would be allowed to abide by local policies/standards versus FBI policies and what level of information would be reported to the City. Additionally, the resolution appears to be "pro FBI" and weakens local laws.

Members and OPD Command staff discussed ways to address the limited reporting details in the annual report and how to more explicitly note that OPD participants would abide by local policies first and foremost when in conflict.

Many noted their concern with the information that was published recently in the White paper referenced above in that it highlighted ways in which the FBVI abused its authority in JTTF cases around the country and misled local law enforcement agencies.

The group agreed to have the Ad hoc group meet with OPD leadership to continue to refine the MOU and Resolution.

7. Adjournment

The meeting adjourned at 7pm.

CITY OF OAKLAND

OAKLAND FIRE DEPARTMENT

DATA COLLECTION AND USE POLICY FOR WILDFIRE DISTRICT AND FIRE SAFETY INSPECTIONS

Purpose

The City of Oakland, Fire Department is transitioning to a new inspection and permitting database called Accela. This transition involves moving from paper/pen documentation to compiling inspection data with electronic devices (iPads and iPhones). An essential piece of this conversion includes the documentation of inspections with photo images collected with electronic devices.

By capturing images of the property/site at the time of inspection, we can document Compliance or Non-Compliance, ensure inspections are completed in accordance to inspection requirements, respond to complaints, use photos for inspection training and provide transparent inspection data to registered property owners and their authorized agents.

Authorized Use

Use of the data collected from Fire Department inspections are limited to:

a) Determination of inspection status results
b) Permit issuance
c) Quality assurance verification
d) Review of inspection record
e) Fire Department inspection training

Data Collection

Data is collected with handheld electronic devices using an Accela approved third-party app (CityGov App) which is downloaded onto the devices. The app will query the Accela database to retrieve inspections based on the search criteria entered by the inspector (station, district, date or date range) and return the inspection list to be completed. The inspector collects data by updating the inspection checklist with data and images related to the inspection checklist item. Once the inspection is complete, the inspection data is submitted from the app to Accela. The app does not store any data but will hold the inspection in its queue to upload to Accela if there is not WiFi connection to submit. Once the queue is cleared, the data can only be accessed in the Accela database.

Photos taken with the handheld device are automatically stored to the device photo log. This log is deleted on a regular basis to provide storage capacity for future inspections. One compliant inspection requires the need to document at least 5 photos and an unlimited number of photos to document non-Compliance.

Accela has a citizen facing portal called Accela Citizen Access (ACA). As part of the online registration process, the applicant must e-mail a copy of their state issued ID to verify their identity against the assessor record of ownership. This information is sent to a shared e-mail account used for Accela support.

Data Access

DATA COLLECTION AND USE POLICY FOR WILDFIRE DISTRICT AND FIRE SAFETY INSPECTIONS

Access to the data collected is limited to employees of the City (City of Oakland) who have active user credentials to log into the Accela database and registered users who have provided proper documentation to indicate a need or a right to see the data. Users have a unique username and password.

Data collected and stored in Accela can be viewed by users in all departments that have active Accela credentials and have access rights.

Data Protection

Data collected for ACA registration is not stored or printed. Once authorization for access has been reviewed and granted or denied, the information is deleted. The City operates "secure data networks' protected by industry standard firewalls and password protection systems. Only authorized individuals have access to the information provided by our users.

Data collected for inspection purposes are stored in the Accela database. This information is kept indefinitely as archival information that may be retrieved for future inspection reports or inspection review. Only person(s) with an active user credential can access the data. The Accela database also has a visible audit log to track changes to the inspection checklist and record. The log documents user, date, time of access and what was changed. The log is visible to all users but cannot be altered or changed.

Accela is a FISMA-NIST (Federal Information Security Management Act--National Institute of Standards and Technology) compliant provider and incorporates security and privacy into the framework of their cloud-based government solutions.

Data Retention

Data collected from inspections are stored indefinitely within the Accela database.

Data collected for ACA registration is not stored. The information is deleted immediately after verification for registration purposes.

Public Access

ACA provides a public facing portal. To provide transparency, any public user may access the ACA portal to gain general information about a property and inspections. By searching an address or parcel number, a public user can check for inspection schedule date and see general inspection results such as Compliant, Non-Compliant or No Access.

If the user has been verified and registration enabled, the user will be able to access detailed information on their records such as photos, letters and fees associated with their property. The verified owner may authorize agents to have access to this information.

The public may also make a public records request. The Fire Department will release information according to the policies set forth by the Public Records Act.

DATA COLLECTION AND USE POLICY FOR WILDFIRE DISTRICT AND FIRE SAFETY INSPECTIONS

Third Party Data Sharing

Other City departments using the Accela database or individuals that have been given Accela credentials will have access to Fire records. As citywide direction to move toward interdepartmental transparency, departments using Accela have read-only access to all other department records in Accela that are not of a sensitive nature.

Training

Annual training is provided to staff using Accela and the inspection app as well as regular training sessions scheduled as needed throughout the year. The trainings focus on an overview of the inspection app and Accela system related to the user group being trained.

Auditing and Oversight

Adherence to the City's Electronic Media Policy as well as the Rules and Regulations set forth by the Oakland Fire Department is expected of personnel with access to data and records collected by the Fire Department. Reported violations will be investigated accordingly.

Maintenance

Data collected will be stored and maintained by Accela in the cloud.

Questions or comments concerning the Collection and Use of Digital Images for Wildfire District and Fire Safety Inspections should be directed to the Assistant Fire Marshal, Emmanuel Watson via e-mail to ewatson@oaklandca.gov or phone at (510) 238-6559.

CITY OF OAKLAND

OAKLAND FIRE DEPARTMENT

SURVEILLANCE IMPACT STATEMENT FOR WILDFIRE DISTRICT AND FIRE SAFETY INSPECTIONS

Information Describing the Technology and How It Works

The Oakland Fire Department (OFD) is transitioning to a new inspection and permitting database called Accela which has been used by the Planning and Building Department for several years. This transition involves moving from paper/pen documentation to compiling inspection data with electronic devices (iPads and iPhones). An essential piece of this conversion includes the documentation of inspections with photo images collected with electronic devices. By capturing images of the property/site at the time of inspection, OFD can document Compliance or Non-Compliance, ensure inspections are completed in accordance to inspection requirements, respond to complaints, use photos for inspection training and provide transparent inspection data to registered property owners and their authorized agents.

Digital images of the inspection site and status at the time of the inspection allows OFD to compile an accurate account of the inspection details. This information can then be reviewed to ensure quality inspection and training; and give a transparent account of the inspection. In combination with the use of the citizen facing portal called ACA (Accela Citizen Access), a registered user can access the record details in the Accela database. This project is a complete renovation of the current manual inspection system to the use of new software and hardware to document inspection details with real time data. The technology will provide clearer documentation of the inspections completed. It also allows inspection documentation to take place much more quickly and be linked to other vital information about the property through the Accela system.

Locations Where, and Situations in which the Technology May Be Deployed

OFD began using the technology in May of 2018 to process vegetation inspections in the Wildfire Protection areas of Oakland (predominantly in the hills above Highway 580). These inspections are completed by firefighters and vegetation inspectors on an annual basis. The technology was deployed out of the Fire Marshal's office with joint staff from the Fire Prevention Bureau and Fire Department command staff. The technology is used daily by the engine company staff and inspectors from the Fire Prevention Bureau to document scheduled inspections or complaints.

OFD is in the process of converting all of its fire inspections to the Accela system which will mean that any code, commercial, or other type of inspection will be tracked and stored in this system. This will create efficiencies that will improve fire safety citywide by allowing for more inspections to occur on an annual basis and will help identify problem properties where an elevated fire hazard may exist. Fire Department personnel including but not limited to firefighters and inspectors will be involved in deployment and use of the technology.

CITY OF OAKLAND

OAKLAND FIRE DEPARTMENT

SURVEILLANCE IMPACT STATEMENT FOR WILDFIRE DISTRICT AND FIRE SAFETY INSPECTIONS

Potential Impact on Civil Liberties & Privacy

Vegetation inspections conducted in the High Fire Severity zones require the use of digital devices (iPad or iPhone) to collect information and digital images of property that is not typically seen from normal street views. Photos taken during vegetation inspections will include images taken around a building or residence to document Compliance/Non-Compliance taken; and images of the status of vacant lots at the time of inspection. During Vegetation inspections, photos are only taken of the exterior of the structure, and vegetation on the parcel being inspected. No photos will be taken inside homes during this inspection process.

For Fire Code Commercial Building and Commercial Occupancy Inspections, photos are taken inside and around the structure to document compliance or non-compliance with the Fire Code. The areas being inspected and photographed are areas that are accessible to the public or are common areas of commercial residential occupancies (Apartments, Condominiums, Hotels, etc.). We do not enter or photograph inside individual residential units during inspections. The only time we would have the need to enter and photograph inside a living space for Fire Code related infractions is on a case by case basis outside of a routine inspection.

This information will be stored in the Accela database to document the inspections completed by the Fire Department.

Mitigations

Access to this data is limited to users with active credentials in Accela and verified property owners and their authorized agents through ACA. All data collected will be stored in the Accela database. All departments using the Accela database will have limited access, dependent on credentials, to each department's dataset. Access is limited to users with active credentials and there is regular review of users by departmental administrators.

ACA registration process includes a verification of the applicant against the assessor record to ensure only the property owner or their agent can have access to the stored photos.

Data Types and Sources

The CityGov app has been loaded onto each device and is used to collect data and images during the inspections. This application is helpful in that it can capture the data, even when an inspector's tablet is not connected to the internet as is often the case in remote areas of the Wildfire Prevention District. The inspector will use the CityGov app to go through the associated checklist and enter the data or take photos. The CityGov app processes the checklist entries to determine the inspection result. The results and photos are uploaded into Accela. The Accela database will store all the data collected. The information is processed and digitally sent to the Accela database. The CityGov app does not store any of the data collected, once the data is sent to Accela, the data collected cannot be accessed on the CityGov app.

CITY OF OAKLAND

OAKLAND FIRE DEPARTMENT

SURVEILLANCE IMPACT STATEMENT FOR WILDFIRE DISTRICT AND FIRE SAFETY INSPECTIONS

The Accela system does allow Data Sharing with other City Departments (primarily Building and Planning) with access to the Accela Information and digital images are collected by

Data Security

Data collected for ACA registration is not stored or printed. Once authorization for access has been reviewed and granted or denied, the information is deleted. The City operates "secure data networks' protected by industry standard firewalls and password protection systems. Only authorized individuals have access to the information provided by our users.

Data collected for inspection purposes are stored in the Accela database. This information is kept indefinitely as archival information that may be retrieved for future inspection reports or inspection review. Only person(s) with an active user credential can access the data. The Accela database also has a visible audit log to track changes to the inspection checklist and record. The log documents user, date, time of access and what was changed. The log is visible to all users but cannot be altered or changed.

Accela is a FISMA-NIST (Federal Information Security Management Act--National Institute of Standards and Technology) compliant provider and incorporates security and privacy into the framework of their cloud-based government solutions.

Fiscal Cost

Third Party Dependence

Other City departments using the Accela database or individuals that have been given Accela credentials will have access to Fire records. As citywide direction to move toward interdepartmental transparency, departments using Accela have read-only access to all other department records in Accela that are not of a sensitive nature.

Alternatives Considered

Non-Surveillance technology was used for many years during these inspections but could not accurately document the status of property at the time of the inspection. This lead to misunderstandings for property owners about what needed to be mitigated on their property which had the potential to lead to fines charged for re-inspection of non-compliant properties. Additionally, auditing of the quality of inspections was difficult as there was no photographic record of what the inspector witnessed for a supervisor to review without visiting the property. Inputting records into a desktop, sometimes hours after an inspection occurred, also created inefficiencies in the processing of inspection results, bills for re-inspection being sent late, or non-compliant owners being overlooked causing an increase in fire hazards.

Track Record of Other Entities

In researching different Automated Inspection Systems, OFD reviewed other jurisdictions

and systems and found the system that Roseville, CA used was the most promising. An added benefit was the fact that the City already has Accela in place in the Planning and Building Department. During the build-out phase, OFD found that certain features of Accela limited its effectiveness in the field, in particular when there was no internet connection. The CityGov application on top of the Accela database fixed many of those user problems creating efficiency.

Questions or comments concerning the Collection and Use of Digital Images for Wildfire District and Fire Safety Inspections should be directed to the Assistant Fire Marshal, Emmanuel Watson via e-mail to ewatson@oaklandca.gov or phone at (510) 238-6559.

CA State Fire Code section relating to Right to Entry

materials, methods of construction or other requirements, the most restrictive shall govern.

[A] 102.11 Other laws. The provisions of this code shall not be deemed to nullify any provisions of local, state or federal law.

[A] 102.12 Application of references. References to chapter or section numbers, or to provisions not specifically identified by number, shall be construed to refer to such chapter, section or provision of this code.

PART 2—ADMINISTRATIVE PROVISIONS

SECTION 103
DEPARTMENT OF FIRE PREVENTION

[A] 103.1 General. The department of fire prevention is established within the jurisdiction under the direction of the fire code official. The function of the department shall be the

SECTION 104
GENERAL AUTHORITY AND RESPONSIBILITIES

[A] 104.1 General. The fire code official is hereby authorized to enforce the provisions of this code and shall have the authority to render interpretations of this code, and to adopt policies, procedures, rules and regulations in order to clarify the application of its provisions. Such interpretations, policies, procedures, rules and regulations shall be in compliance with the intent and purpose of this code and shall not have the effect of waiving requirements specifically provided for in this code.

[A] 104.2 Applications and permits. The fire code official is authorized to receive applications, review construction documents and issue permits for construction regulated by this code, issue permits for operations regulated by this code, inspect the premises for which such permits have been issued and enforce compliance with the provisions of this code.

[A] 104.3 Right of entry. Where it is necessary to make an inspection to enforce the provisions of this code, or where the

fire code official has reasonable cause to believe that there exists in a building or upon any premises any conditions or violations of this code that make the building or premises unsafe, dangerous or hazardous, the fire code official shall have the authority to enter the building or premises at all reasonable times to inspect or to perform the duties imposed upon the fire code official by this code. If such building or premises is occupied, the fire code official shall present credentials to the occupant and request entry. If such building or premises is unoccupied, the fire code official shall first make a reasonable effort to locate the owner, the owner's authorized agent or other person having charge or control of the building or premises and request entry. If entry is refused, the fire code official has recourse to every remedy provided by law to secure entry.

[A] 104.3.1 Warrant. Where the fire code official has first obtained a proper inspection warrant or other remedy provided by law to secure entry, an owner, the owner's authorized agent or occupant or person having charge, care or control of the building or premises shall not fail or neglect, after proper request is made as herein provided, to permit entry therein by the fire code official for the purpose of inspection and examination pursuant to this code.

shall be constructed and installed in accordance with such approval.

[A] 104.7.1 Material and equipment reuse. Materials, equipment and devices shall not be reused or reinstalled unless such elements have been reconditioned, tested and placed in good and proper working condition and approved.

[A] 104.7.2 Technical assistance. To determine the acceptability of technologies, processes, products, facilities, materials and uses attending the design, operation or use of a building or premises subject to inspection by the fire code official, the fire code official is authorized to require the owner or owner's authorized agent to provide, without charge to the jurisdiction, a technical opinion and report. The opinion and report shall be prepared by a qualified engineer, specialist, laboratory or fire safety specialty organization acceptable to the fire code official and shall analyze the fire safety properties of the design, operation or use of the building or premises and the facilities and appurtenances situated thereon, to recommend necessary changes. The fire code official is authorized to require design submittals to be prepared by, and bear the stamp of, a registered design professional.

FOR OFFICIAL USE ONLY

JOINT TERRORISM TASK FORCE

STANDARD MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATIONI

AND

THE OAKLAND POLICE DEPARTMENT

PREAMBLE

The policy of the United States with regard to domestic and international terrorism is to deter, defeat and respond vigorously to all terrorist attacks on out territory and against our citizens, or facilities. Within the United States, the Department of Justice, acting through the Federal Bureau of Investigation (FBI), is the lead agency domestically for the counterterrorism effort.

In order to ensure that there is a robust capability to deter, defeat and respond vigorously to terrorism in the U.S. interest, the FBI recognizes the need for all federal, state, local and tribal agencies that are involved in fighting terrorism to coordinate and share information and resources. To that end, the FBI believes that the creation of the FBI National Joint Terrorism Task Force (NJTTF) and Joint Terrorism Task Forces (JTTFs) embodies the objectives of the U.S. policy on counterterrorism as set forth in Presidential Directives.

FBI policy for the NJTTF and JTTFs is to provide a vehicle to facilitate sharing FBI information with the intelligence and law enforcement communities to protect the United States against threats to our national security, including international terrorism, and thereby improve the effectiveness of law enforcement, consistent with the protection of classified or otherwise sensitive intelligence and law enforcement information, including sources and methods. All NJTTF and JTTF operational and investigative activity, including the collection, retention and dissemination of personal information, will be conducted in a manner that protects and preserves the constitutional rights and civil liberties of all persons in the United States.

This Memorandum of Understanding (MOU) shall serve to establish the parameters for the detail of employees (Detailees or members) from the Participating Agency to the FBI-led JTTF's in selected locations around the United States.

I. PURPOSE

A. The purpose of this MOU is to outline the mission of the JTTF, and to formalize the relationship between the FBI and the Participating Agency; in order to maximize cooperation and to create a cohesive unit cable of addressing the most complex terrorism investigations.

B. The MOU specifically represents the agreement between the FBI and the Participating Agency, which will govern the process by which employees of the Participating Agency are detailed to work with the FBI as part of the JTTF.

C. The MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law of otherwise by any third party against the parties, their parent agencies, the U.S., or the officers employees, agents or other associated personnel thereof.

II. MISSION

The mission of the JTTF is to leverage the collective resources of the member agencies for the prevention, preemption, deterrence and investigation of terrorist acts that affect United States interests and to disrupt and prevent terrorist acts and apprehend individuals who may commit or plain to commit such acts. To further this mission, the JTTF shall serve as a means to facilitate information sharing amount JTTF members.

III. AUTHORITY

Pursuant to 28U.S.C. §533, 28 C.F.R. §0.85. Executive Order 12333, Presidential Decision Directive (PDD) 39, PDD 62 and pending approval of National Security Presidential Decision Directive (NSPD) 46 and Homeland Security Presidential Directive (HSPD) 15, the FBI is authorized to coordinate an intelligence, investigative and operational response to terrorism. By virtue of that same authority, the FBI formed the JTTFs composed of other federal, state, local and tribal law enforcement agencies acting in support of the above listed statutory and regulatory provisions.

[Participating agencies may include applicable authority for entering into this MOU.]

IV. CONTROLLING DOCUMENTS

A. Since the JTTF operates under the authority of the Attorney General of the United States, all JTTF participants must adhere to applicable Attorney General's Guidelines and directives, to include the following; as amended or supplemented;

1. Attorney General's Guidelines on General Crimes, Racketeering enterprise and Terrorism Enterprise Investigations;

2. Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection;

3. Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations;

4. Attorney General's Guidelines Regarding Prompt Handling of Reports of Possible Criminal Activity Involving Foreign Intelligence Sources;

5. Attorney General's Memorandum dated march 6, 2002, titled "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI;

6. Attorney General's Guidelines Regarding the Use of Confidential Informants;

7. Attorney General's Guidelines on the Development and Operation of FBI Criminal Formants and Cooperative Witnesses in Extraterritorial Jurisdictions;

8. Attorney General's Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Court of a Criminal Investigation; and

9. Memorandum of the Deputy attorney General and the FBI Director re: Field Guidance on Intelligence Sharing Procedures for [Foreign Intelligence] and [Foreign Counterintelligence] Investigations (December 24, 2002).

B. All guidance on investigative matters handled by the JTTF will be issued by the Attorney General and the FBI. The FBI will provide copies of the above-listed guidelines and any other applicable policies for referenced and review to all JTTF members. Notwithstanding the above, this MOU does not alter or abrogate existing directives or policies regarding the conduct of investigations or the use of special investigative techniques or controlled informants. The FBI agrees to conduct periodic briefings of the member agencies of the JTTF subsequent to execution of this agreement.

V. STRUCTURE AND MANAGEMENT OF THE TASK FORCE

A. MEMBERS

1. Each JTTF shall consist of a combined body of sworn and non-sworn personnel from the FBI and each Participating Agency. This MOU shall apply to Participating Agencies that join the JTTF subsequent to execution of this agreement.

B. PROGRAM MANAGEMENT, DIRECTION AND SUPERVISION

1. In order to comply with Presidential Directives, the policy and program management of the JTTFs is the responsibility of FBI Headquarters (FBIHQ). The overall commander of each individual JTTF will be the Special Agent in Charge (SAC) or Assistant Director in Charge (ADIC), if assigned, of the FBI's local Field Division The operational chain of command beginning at the highest level, in each FBI Field Division will be as follows" ADIC if assigned, SAC, Assistant Special Agent in Charge (ASAC), and Supervisory Special Agent [JTTF Supervisor].

2. Each FBI ADIC/SAC, through his or her chain-of-command, is responsible for administrative and operational matters directly associated with the Division's JTTF(s). Operational activities will be supervised by FBI JTTF Supervisors. Staffing issues are the responsibility of the FBI chain of command.

3. All investigations opened and conducted by the JTTF must be conducted in conformance with FBI policy, to include the above stated Controlling Documents. Each FBI ADIC/SAC, through his or her chain-of-command, will ensure that all investigations are properly documented on FBI form in accordance with FBI rules and regulations. Any operational problems will be resolved at the field office level. Any problems not resolved at the field office level will be submitted to each agency's headquarters for resolution.

4. Each Participating Agency representative will report to his or her respective agency for personnel administrative matters. Each Participating Agency shall be responsible for the pay, overtime, leave, performance appraisals, and other personnel matters relating to its employees detailed to JTTFs. As discussed later herein a Paragraph XI, the FBI and Participating Agency may provide for overtime reimbursement by the FBI by separate written agreement.

5. Each JTTF member will be subject to the personnel rules, regulations, laws and policies applicable to employees of his or her respective agency and also will adhere to the FBI's ethical standards and will be subject to the Supplemental Standards of Ethical Conduct for employees of the Department of justice. Where there is a conflict between the standards or requirements of the greatest organizational protection of benefit will apply, unless the organizations jointly resolve the conflict otherwise.

6. JTTF members are subject to removal from the JTTF by the FBI for violation of any provision of this MOU, the FBI's ethical standards, the Supplemental Standards of Ethical Conduct for employees of the Department of Justice, or other applicable agreements, rules and regulations.

7. The FBI maintains oversight and review responsibility of the JTTFs. In the event of any FBI inquiry into JTTF activities by an investigative or administrative body, including but not limited to, the FBI's Office of Professional Responsibility or the FBI's Inspection Division, each Participating Agency representative to the JTTF, may be subject to interview by the FBI.

C. PHYSICAL LOCATION AND SUPPORT

1. The FBI will provide office space for all JTTF members and support staff. In addition, the FBI will provide all necessary secretarial, clerical, automation and technical support for the JTTF in accordance with FBI guidelines and procedures. The FBI will provide all furniture and office equipment. Participating agencies may bring office equipment furniture into FBI space with the approval of the FBI JTTF Supervisor and in compliance with FBI regulations.

2. The introduction of office equipment and furniture into FBI space by participating agencies is discouraged, as any such material is subject to examination for technical compromise, which may result in its being damaged or destroyed

VI. SECURITY PROGRAM

A. CLEARANCES

1. State, local and tribal members of the JTTFs, as well as appropriate supervisory personnel responsible for these individuals, must apply for and receive a Top Secret/Sensitive Compartmental Information (TS/SCI) Security Clearance granted by the FBI. JTTF members from other federal agencies must obtain a Top Secret/SCI clearance from their agency and have this information passed to the FBI. No one will have access to sensitive or classified documents or material or FBI space without a valid security clearance and the necessary "need-to-know." Pursuant to the provision of Section 1.2 of the Executive Order 12968, Detailees are required to have signed a non-disclosure agreement approved by the FBI's Security Division. Pursuant to federal law, JTTF members are strictly for bidden from disclosing any classified information to individuals who do not possess the appropriate security clearance and the need to know.

2. All JTTF management personnel must ensure that each participating JTTF officer or agent undertakes all necessary steps to obtain a TS/SCI clearance. Conversion of FBI counterterrorism and JTTF spaces to Sensitive Compartmented Information Facilities (SCIFs) is underway. This will require that all JTTF task force officers enhance their clearances to TS/SCI (SI,TK, Gamma, HCS-P).

3. Federal agency task force officers should contact their Security Officers and request and obtain the following SCI Clearances; SI, TK, Gamma and HCS-P. If the parent agency refuses or is unable to provide the appropriate clearances, the FBI will request the task force officer's security file. If provided, the FBI will adjudicate the SCI clearances. This action may not involve a prohibitively long process and should be avoided.

4. Each Participating Agency fully understands that its personnel detailed to the JTTF' are not permitted to discuss official JTTF business with supervisors who are not members of the JTTF unless the supervisor possesses the appropriate security

clearance and the dissemination or discussion is specifically approved the FBI JTTF Supervisor. Participating Agency heads will be briefed regarding JTTF matters by the SAC or ADIC, as appropriate through established JTTF executive Board meeting.

5. In accordance with the Director of Central Intelligence Directive (DCID) 6/4, entitled Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI), the FBI will implement protocols to ensure Special Agent (SA) and Task Force Officers (TFO) assigned to Joint Terrorism task Forces (JTTF) in the field and the National Joint Terrorism Task Force (NJTTF) at FBI Headquarters – Liberty Crossing 1, are in compliance with stated directive. In order to comply with DCID 6/4, all JTTF personnel, including FBI and non FBI JTTF members and contractors who perform functions requiring access to FBI classified data networks and space, will be given counter-intelligence focused on polygraphs. The FBI will recognize polygraph examination meets the PSPP requirements.

6. All JTTF members must agree to submit to counter-intelligence focused polygraphs as part of the process for obtaining and retaining a Top Secret Security Clearance.

B. RESTRICTIONS ON ELECTRONIC EQUIPTMENT

Personally owned Portable Electronic Devices (PEDs) including, but not limited to, personal digital assistance, Blackberry devices, cellular telephones and two-way pagers are prohibited in FBI space unless properly approved. No personally owned electronic devices are permitted to operate within SCIF's as outlined in DCI Directive 6/9 and existing Bureau policy. All other non-FBI owned information technology and systems (such as computers, printers, fax machines, copers, PEDs, cameras and medical including diskettes, CDs, tapes) require FBI approval prior to introduction, operation, connection or removal from FBI spaces to include SCIFs' Additionally, if approved by the FBI Security Officer, these systems must operate in compliance with the FBI's policies, guidelines and procedures.

VII. DEPUTATION

Non-federal members of the JTTF who are subject to a background inquiry and are sworn law enforcement officers will be federally deputized while detailed to the JTTF. The FBI will secure the required authorization for the deputation. Deputation of these individuals will ensure that they are able to assist fully in investigations in compliance with applicable federal statutes. On occasion, investigations may be conducted outside

of the JTTF's assigned territory. Deputation will allow non-federal members of the JTTF to exercise federal law enforcement authority throughout the United States.

Under the terms of this MOU, all Participating Agencies agree that non-sworn detailed to the JTTF will not: (1) participate in law enforcement activities, (2) carry a weapon or (3) participate in the execution of search/arrest warrants.

VII. STAFFING COMMITMENT

A. In view of the need for security clearances and continuity of investigations, all personnel detained to the JTTF should be expected to be detained for the period of at least two (2) years. This MOU imposes no maximum limit as to the time that any individual may remain a member of the JTTF. All non-FBI members of the JTTF must adhere to the same rules and regulations as FBI employees with regard to conduct and activities while in FBI space, while operating FBI vehicles, and while conducting JTTF business. All Task Force members detained from other federal agencies are responsible for maintaining an appropriate case load, as directed by JTTF management.

B. All investigators detailed to the JTTF will be designed either full-time or part-time. The operational needs of the JTTF require that any assignments to special details, or duties outside of the JTTF to full time JTTF members be coordinated with the FBI JTTF Supervisor. Though each JTTF member will report to his or her respective Participating Agency for personnel matters, he or she will coordinate leave with the JTTF's FBI JTTF Supervisor.

C. During periods of heightened threats and emergencies, the JTTFs may be expected to operate 24 hours a day, seven days per week, for extended periods of time. To function properly, the JTTF depends upon the unique contributions of each Participating Agency. Accordingly, during these periods, each Participating Agency member will be expected to be available to support JTTF activities

IX. RECORDS, REPORTS AND INFORMATION SHARING

A. All JTTF materials and investigative records, including any Memorandum of Understanding, originate with, belong to, and will be maintained by the FBI. All investigative reports will be prepared by JTTF personnel solely by the FBI and may not be removed from FBI space with the approval of the JTTF Supervisor. Dissemination, access or other use of JTTF records will be in accordance with Federal law, Executive Orders, and Department of Justice and FBI regulations and policy, including the dissemination and information sharing provisions of the FBI Intelligence Policy Manual. As FBI records, they may be disclosed only with FBI permission and only in conformance with the provisions of federal laws and regulations, including the Freedom of Information Act, 5 U.S.C. Section 552, and the Privacy Action of 1974, 5 U.S.C. Section 552a, as well as applicable civil and

criminal discovery privileges. This policy includes any disclosure of FBI information, including JTTF materials and investigative records, to employees and officials of a Participating Agency who are not members of a JTTF which must be approved by the JTTF supervisor. All electronic records and information, including, but not limited to, systems, databases and media, are also regulated by FBI policy. JTTF members may request approval to disseminate FBI information from the JTTF Supervisor.

B. Each Participating Agency agrees to have its Detailees to the JTTF execute an FD-868, or a similar form approved by the FBI. This action obligates the Detailee, who is accepting a position of special trust in being granted access to classified and otherwise sensitive information as part of the JTTF, to be bound by prepublication review to protect against the unauthorized disclosure of such information,

C. The participation of other federal, state, local and tribal partners on the JTTF us critical to the long term success of the endeavor. Articulating the level of effort for these partnership is a key measure of the JTTF's performance. According, all task force members will be required to record their workload in the Time Utilization Recordkeeping (TURK) system used by the FBI.

X. COORDINATION

A. The Participating Agency agrees to not knowingly act unilaterally on any matter affecting the JTTF without first coordinating with the FBI. The parties agree that matters designated to be handled by the JTTF shall not knowingly be subject to non-JTTF or non-FBI intelligence, law enforcement and operation actions will be coordinated and cooperatively carried out within the JTTFs.

B. JTTF criminal investigative procedures will conform to the requirements for federal prosecution. It is expected that the appropriate United States Attorney in consultation with the FBI and affected JTTF partners, will determine on a case-by-case basis whether the prosecution of cases will be at the federal or state level, based upon which would better advance the interests of justice.

XI. FUNDING

This MOU is not an obligation or commitment of funds, not a basis for transfer of funds. Even where one party has agreed (or later does agree) to assume a particular financial responsibility, written agreement must be obtained before incurring an expense expected to be assumed by another party. All obligations of an expenditures by the parties are subject to their respective budgetary and fiscal processes and availability of funds pursuant to all laws, regulations and policies applicable thereto. The parties acknowledge that there is no intimation, promise or guarantee that funds will be available in future years. The FBI and

the Participating Agency may enter into a separate agreement to reimburse the Participating Agency' for approved overtime expenses.

XII. TRAVEL

All JTTF-related travel of non-FBI personnel requires the approval of the appropriate JTTF Supervisor and Participating Agency authorization prior to travel. In order to avoid delay in operation travel, the Participating Agency will provide general travel authority to all of its participating employees for the duration of the employee's membership in the JTTFs. For domestic travel, each agency member will be responsible for appropriate notifications within his or her own agency, as well as standard FBI travel approvals and notification. The FBI will obtain FBIHQ authorization and country clearances for all JTTF members who are required to travel outside the United States. As noted above, the appropriate security clearance must be obtained prior to any international travel. The FBI will pay costs for travel of all members of the JTTFs to conduct investigations outside of the JTTF's assigned territory.

XIII. VEHICLES AND EQUIPMENT

A. In furtherance of this MOU, employees of the Participating Agency may be permitted to drive FBI owned or leased vehicles for surveillance, case management and investigation in connection with any JTTF investigation. FBI vehicles must only be used for official JTTF business and only in accordance with applicable FBI rules and regulations.

B. *[non-Federal entities only]* Any civil liability arising from the use of any FBI owned or leased vehicle by a Participating Agency task force member while engaged in any conduct other than his or her official duties and assignments under this MOU shall be the responsibility of the Participating Agency. The Participating Agency will indemnity and hold harmless the FBI and the United State for any claim for property damage or personal injury arising from any use of any FBI owned or leased vehicle by a Participating Agency JTTF member which is outside of the scope of his or her official duties and assignments under this MOU.

C. For official inventory purpose, all JTTF equipment including badges, credentials and other form of JTTF identification subject to FBI property inventory requirements will be produced by each JTTF member upon request. At the completion of the member's assignment on the JTTF, or upon withdrawal or termination of the Participating Agency from the JTTF, all equipment will be returned to the supplying agency.

XIV. FORFEITURE

The FBI shall be responsible for the processing of assets seized for federal forfeiture in conjunction with JTTF operations, as provided by these rules and regulations. Asset

forfeitures will be conducted in accordance with federal law and the rules and regulations set forth by the U.S. Department of Justice and the FBI. Forfeitures attributable to JTTF investigations may be distributed among the Participating Agency in JTTF-related operations at the discretion of the FBI.

XV. HUMAN SOURCES

A. All human sources developed through the JTTF will be handled in accordance with the Attorney General and the FBI's Guidelines, policies and procedures.

B. All human sources developed through the JTTF investigation shall be operated with all appropriate FBI suitability paperwork completed prior to use. All source debriefings or written products of information obtained from any human source will use FBI document format and handling procedures.

C. The FBI, as permitted by federal law, agrees to pay reasonable and necessary human source expenses incurred by the JTTF. All expenses must be approved by the FBI before they are incurred. No payments may be made to JTTF human sources without prior FBI approval.

XVI. MEDICAL

A. All Participating Agencies will ensure that detailed JTTF members are medically qualified according to their agencies' standards to perform law enforcement duties, functions and responsibilities.

B. To ensure protection for purposes of the Federal Employees' Compensation Act (FECA), JTTF members should be detailed to the FBI consistent with the provisions of the Intergovernmental Personnel Act (IPA), 5 U.S.C. § 337(d). This Act stipulates that "[a] State of local government employee who is given an appointment in a Federal agency for the period of the assignment or who is on detail to a Federal agency and who suffers disability or dies as a result of a personal injury sustained while in the performance of his duty during the assignment shall be treated . . . as though he were an employee as defined by section 8101 of this title who has sustained the injury in the performance of duty." Other provisions of federal law may extend FECA benefits in more limited circumstances. The Department of Labor's Office of Workers' Compensation Program is charged with making FECA coverage determinations and is available to provide guidance concerning specific circumstances.

XVII. TRAINING

All JTTF members are required to attend FBI legal training in compliance with FBI regulations and any other training deemed necessary by the FBI chain of command. The FBI is responsible for the costs of such training. The Participating Agency will bear

the costs of any training required of its own employees detailed to the JTTF.

XVIII. DEADLY FORCE AND SHOOTING INCIDENT POLICIES

Members of the JTTF will follow their own agency's policy concerning use of deadly force.

XIX. DEPARTMENT OF DEFENSE COMPONENTS

The Posse Comitatus Act, 18 U.S.C. § 1385, prohibits the Army and Air Force (Department of Defense regulations now restrict the activities of all branches or components of the Armed Services under this Act) from being used as a posse comitatus or otherwise to execute the laws entrusted to civilian law enforcement authorities. The restrictions of the Act do not apply to civilian employees of the Department of Defense who are not acting under the direct command and control of a military officer. Other statutory provisions specifically authorize certain indirect and direct assistance and participation by the military in specified law enforcement functions and activities. All Department of Defense components (except strictly civilian components not acting under direct command and control of a military officer) who enter into this agreement, shall comply with all Department of Defense regulations and statutory authorities (describing restrictions, authorizations and conditions in support of law enforcement) including but not limited to Department of Defense Directives 5525.5, and 3025.15, Chapter 18 of Title 10 of the United States Code dealing with military support for civilian law enforcement agencies and any other or subsequent rules, regulations and laws that any address this topic or that may amend, or modify any of the above provisions. This MOU shall not be construed to authorize any additional or greater authority (than already described) for Department of defense components to act in support of law enforcement activities.

XX. MEDIA

All media releases will be mutually agreed upon and jointly handled by the member Participating Agencies of the appropriate JTTF. Press releases will confirm to DOJ Guidelines regarding press releases. No press release will be issued without prior FBI approval.

XXI. LIABILITY

The Participating Agency acknowledges that financial and civil liability, if any and in accordance with applicable law, for the acts and omissions of each employee detailed to the JTTF remains vested with his or her employing agency. However, the Department of Justice (DOJ) may, in its discretion determine on a case-by-case basis that an individual should be afforded legal representation, legal defense or indemnification of a civil judgment, pursuant to federal law and DOJ policy and regulations.

A. COMMON LAW TORT CLAIMS

1. Congress has provided that the exclusive remedy for the negligent or wrongful act or omission of any employee of the U.S Government, acting within the scope of his or her employment, shall be an action against the United States under FTCA, 28 U.S.C. § 1346(b) and §§ 2671 – 2680.

2. Nothwithstanding the provisions contained in Article XIII of this MOU, for the limited purpose of defending civil claims arising out of JTTF activity, a state, local or tribal law enforcement officer who has been federally deputized and who is acting within the course and scope of his or her official duties and assignments pursuant to the MOU may be considered an "employee" of the U.S. government, as defined at 28 U.S.C. § 2671. See 5 U.S.C. § 3374(c)(2).

3. Under the Federal employee Liability reform and Tort Compensation Act of 1998 (commonly known as the Westfall Act), 28 U.S.C. § 2679(b)(1), if an employee of the United States is named as a defendant in a civil action, the Attorney General or his or her designee may certify that the defendant acted within the scope of his or her employment at the time of the incident giving rise to the suit. 28 U.S.C. § 2679(d)(2). The United States can then be substituted for the employee as the sole defendant with respect to any tort claims alleged in the action. 28 U.S.C. § 2679(d)(2). If the United States is substituted as defendant, the individual employee is thereby protected from suit on any tor claim arising out of the incident.

4. If the Attorney General declines to certify that an employee was acting within the scope of employment, "the employee may at any time before trial petition the court to find and certify that the employee was acting with the scope of his office or employment." 28 U.SC. § 269(d)(3).

5. Liability for any negligent or willful acts of JTTF members undertaken outside the terms of this MOU will be the sole responsibility of the respective employee and agency involved.

B. CONSTITUTIONAL CLAIMS

1. Liability for violations of federal constitutional law may rest with the individual federal agent of officer pursuant to Bivens v. Six Unknown Names Agents of the Federal Bureau of Narcotics, 403 U.S. 388 (1971) or pursuant to 42 U.S.C. § 1983 for state officers.

2. Federal, state, local and tribal officers enjoy qualified immunity from suit for constitutional torts, “insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.” Harlow v. Fitzgerald 457 U.S. 800 (9182).

3. If a Participating Agency JTTF officer is named as a defendant in his or her individual capacity in a civil action alleging constitutional damages as a result of conduct taken within the course of the JTTF, the officer may request representation by DOJ. 28 C.F.R. §§ 50.15, 50.16.

4. An employee may be provided representation “when the actions for which representation is requested reasonably appears to have performed within the scope of the employee’s employment and the Attorney General, or his or her designee, determines that providing representation would otherwise be in the interest of the United States.” 28 C.F.R. §50.15(a).

5. A JTTF member’s written request for representation should be directed to the Attorney General and provided to the Chief Division Counsel (CDC) of the FBI division coordinating the JTTF. The CDC will forward the representation request to the FBI’s Office of the General Counsel (OGC) together with a letterhead memorandum concerning the factual basis of the lawsuit. FBI’s OGC will then forward the request to the Civil Division of DOJ together with an agency recommendation concerning scope of employment and DOJ representation. 28 C.F.R. §50.15(a)(3).

6. If a JTTF member is found to be liable for a constitutional tort, he or she may request indemnification from DOJ to satisfy and adverse judgment rendered against the employee in his or her individual capacity. 28 C.F.R. § 50.15(c)(4). The criteria for payment are substantially similar to those used to determine whether a federal employee is entitled to DOJ representation under 28 C.F.R. §(a).

7. Determination concerning legal representation and indemnification by the United States are discretionary and are made by DOJ on a case by case basis. The FBI cannot guarantee that the United States will provide legal representation, legal defense, or indemnification to any federal or state employee detailed to the JTTF, and nothing in this Article shall be deemed to create any legal right on the part of any JTTF personnel.

C. EXPRESS RESERVATIONS

1. Nothing in this Article shall be deemed to create an employment relationship between the FBI or the United States and any Participating Agency JTTF member other than for exclusive purposes of the FTCA as outlined herein.

2. The participating agencies do not waive any available defenses and/or limitations on liability. No Participating Agency shall be considered to be an agent of any other Participating Agency.

XXII. DURATION

A. The term of the MOU shall be an indefinite period. The MOU may be terminated at will by any party, provided written notice is provided to the other parties of not less than sixty (60) days. Upon termination of the MOU, all equipment will be returned to the supplying agency(ies). It is understood that the termination of this agreement by any one of the Participating Agencies will have no effect on the agreement between the FBI and all other participating agencies.

B. Notwithstanding this provision, the provisions of Paragraph IX, entitled RECORDS, REPORTS AND INFORMATION SHARING, and Paragraph XXI, entitled LIABILITY, will continue until all potential liabilities have lapsed. Similarly, the inherent disclaimer limitation contained in the EXPRESS RESERVATION provision will survive any termination.

XXIII. AMENDMENTS

This agreement in no manner affects any existing MOUs or agreements with the FBI or any other agency. This agreement may be amended only by mutual written consent of the parties. The modification shall have no force and effect unless such modifications are reduced to writing and signed by an authorized representative of the FBI and the Participating Agency.

OAKLAND POLICE DEPARTMENT

Surveillance Impact Report

For

Mobile Identification Devices

---

1. Mobile Identification Devices (MID) and How they Work

Mobile Identification Devices (MID) are small enough to be handheld, and contains an optical sensor to scan fingerprints and transmit them to look for matches within local databases. The MID uses the Bluetooth radio standard to send a scanned image of a fingerprint to a police vehicle mobile data terminal (MDT), which can connect with special software. The software accesses a regional fingerprint database shared by Alameda and Contra Costa Sheriff's Offices called Cogent Automated Fingerprint Identification System (CAFIS). The MDT software sends the fingerprint digital image to CAFIS where the Almeda and Contra County CAL-ID Mobile Web ID system runs the fingerprint against the CAFIS system to look for matches. The software match process uses a graphic representation of the print as a mathematical model of the relationships between the ridges of the fingerprint image. This mathematical measuring of friction ridges allows the image to be transmitted as a string of numbers the Automated Fingerprint Identification System (AFIS) databases can use.

Search results are sent back to MDTs. If a search result ends in a match with CAFIS, a fingerprint record will appear in the MID with the following:

- Transaction Number;
- Main Number,
- Name on Record;
- Date of Birth (DOB);
- Sex;
- Person File Number (PFN) / Juvenile File Number (JFN); and
- Arrest Booking Photo (if one is on file).

The hit will only return with the record hit (not a list of possible matches); a hit means a 100 percent match. No hits return with the display, "No hit." A "No Hit" means only that the subject's fingerprints are not in the CAFIS database.

2. Proposed Purpose

MIDs allow police to identify individuals who do not possess acceptable forms of identification (e.g. driver's license or passport). Police need to identify (ID) individuals to be cited for an infraction or misdemeanor; arrest and booking into jail is legally required when an acceptable form of ID cannot be obtained. In 2018, there were arrests where 40302(a) or (b)[1] was one of the listed offenses; so far OPD has seen one arrest in 2019 for 40302 (a) or (b). OPD currently takes arrested individuals to the Alameda County Sheriff's Office (ACSO) Santa Rita Jail in Dublin, CA, where they are turned over to ACSO deputies for intake and identification.

Each arrest requires the time (hours) of one or more police officer as well as a significant time (several hours or more) of the individual who may or may not need to be legally arrested. Infractions and several types of misdemeanor do not require custodial arrests and associated jail bookings. The arrest can cause varying levels of stress for individuals and lead to escalations of anger, noncompliance, and even use of force. By providing rapid ID when records exist, MIDs can mitigate these challenges as well as offer other benefits.

Officers may also ID a person who needs immediate medical treatment based on the records available. Its use can also lead to faster communication with relatives to attend a hospital to see their loved ones when time is of the essence. Individuals who could be cited for an infraction or misdemeanor but cannot provide ID can also be saved the burden of transportation back to Oakland after the full arrest and booking process. Furthermore, officers can more efficiently utilize patrol service time in the community.

3. Locations Where, and Situations in which the MID System may be deployed or utilized.

The technology would be provided to patrol officers throughout the five police areas of the City. As noted above, in 2018, there were eight arrests where 40302(a) or (b) was one of the listed offenses; so far OPD has seen one arrest in 2019 for 40302 (a) or (b).

4. Privacy Impact

The privacy risks associated with MID are: 1) personnel could abuse the device to ascertain a person's identify when not justified; or 2) the person's data,

[1] 40302: Whenever any person is arrested for any violation of this code, not declared to be a felony, the arrested person shall be taken without unnecessary delay before a magistrate within the county in which the offense charged is alleged to have been committed and who has jurisdiction of the offense and is nearest or most accessible with reference to the place where the arrest is made in any of the following cases: (a) When the person arrested fails to present both his or her driver's license or other satisfactory evidence of his or her identity and an unobstructed view of his or her full face for examination; (b) When the person arrested refuses to give his or her written promise to appear in court

associated with fingerprints, could be shared intentionally or unintentionally in ways that violate the person's right to privacy. To address the first concern, OPD Department General Order (DGO) I-21 "MOBILE IDENTIFICATION DEVICES" explicitly requires that MID may only be used when the individual provides knowing and voluntary[2] consent (captured via Body-Worn Camera (BWC) video or on a signed consent form[3], and one of the following circumstances exist:

1. Probable causes exists for the subject's arrest; or
2. The subject is to be cited for an infraction or misdemeanor and cannot provide satisfactory evidence of identity.

In terms of a person's data being shared in ways that violate their expectation and / or right to privacy, the MID technology does not store any data – it only searches data that already exists. Fingerprint data is never transferred or stored from existing databases onto MDTs or other OPD data systems.

5. Mitigations

MIDs are designed to not store data but to only access the fingerprint database shared between Alameda and Contra Costa County. Since data is not retained by the MID or police computer, personally identifiable data is not shared inappropriately. DGO I-21 C.3 provides another layer of privacy impact mitigation – in the event that an officer uses the MID with a person's voluntary consent, the officer will use personal a BWC to record the encounter and ensure an evidentiary record.

6. Data Types and Sources

The MID is used to scan an individual's fingerprint. The scan is connected via the MID to a fingerprint databased maintained by ACSO and the Contra Costa Sheriffs Office. The fingerprint images are scanned using algorithms to compare different points on the image of the fingerprint. This system can also connect to arrest records if the algorithm matching software sees a match between a MID-scanned fingerprint image and a fingerprint on file. In this case, the MID will access the arrest record and personal file number from the prior arrest with associated name on file. Alameda County Mobile ID devices use the CAL-ID Mobile WEB ID system to run fingerprint searches against the fingerprint database. MID users must log into the Mobile ID WEB ID systems to use the Mobile ID device and receive search results.

7. Data Security

ACSO's Central Identification Bureau (CIB) manages Alameda County's CAL-ID System infrastructure consisting of an infrastructure of CAL-ID systems, sub-

[2] Officers seeking consent shall tell the subject that they have the right to refuse being identified via MID.
[3] As of the effective date of this order, the form number is TF-2018.

systems and network. The main CAL-ID system is an Automated Fingerprint Identification System (AFIS). CAL-ID includes several supporting systems also referred to as 'sub-systems' that provide additional information and tools to law enforcement. Supporting systems include mugshot and mobile ID systems. Management includes all CAL-ID databases, equipment, system and equipment maintenance, equipment deployment, training and system access. All systems are Criminal Justice Information Service (CJIS)-compliant, meaning that ACSO maintains security controls aimed at ensuring only authorized individuals have access to the fingerprint information. Furthermore, this system is maintained behind a firewall and is housed separate from other ACSO systems and Alameda County internet and data systems.

All users must first complete the Mobile ID User Agreement and receive hands-on training. The agreement is signed by their supervisor and sent to ACSO's CIB for final approval and user account access. When the user signs the Mobile Identification User Agreement, they certify that they have received training, and will abide by all policies.

Any maintenance required of the MID will done by ACSO staff, and requests will be directed to ACSO through the OPD Information Technology Unit.

8. Costs

ACSO will accept all costs to furnish OPD with MID technology. ACSO will also maintain responsibility for maintenance costs.

9. Third Party Dependence

ACSO will provide MID devices to OPD and will accept all costs to furnish OPD with MID devices. The MID devices themselves are made by Cogent (owned by 3M).

10. Alternatives Considered

The alternative to using MIDs for persons that cannot be identified in conditions outlined in DGO I-21.C.1 will be to continue to arrest people who otherwise would not need to be arrested and taken to jail in Dublin, CA for the purpose of identification. In these cases, people will continue to assume the burden of arrest and transport a long distance from Oakland, and police time will continue to be used ineffectively. OPD is not aware of another system for legally identifying persons without acceptable identification.

11. Track Record of Other Entities

MID devices are used by many California city police agencies and county sheriff departments. Cities include:

- Fresno;
- Los Angles;
- San Francisco;
- San Jose;
- Modesto; and
- Pasadena;

Counties include:

- Fresno;
- Kern;
- Los Angeles'
- Marin;
- Santa Clara;
- San Francisco; and
- Stanislaus

Other jurisdictions are using other similar technology:

- The Brentwood Police Department has installed BlueCheck mobile ID systems – a similar type of fingerprint reader, in some police vehicles. These handheld devices also match prints to files maintained by Contra Costa and Alameda counties.
- The San Jose Police Department, in partnership with Santa Clara County, is using BlueCheck, a mobile fingerprinting device from 3M Corporation.
- The L.A. County Sheriff's Office and several L.A. County police departments are also using BlueCheck devices for fingerprint ID.
- Several Alameda County police departments are using the Cogent 3M MIDs, including Berkeley, Hayward, and San Leandro.

DEPARTMENTAL GENERAL ORDER

I-21: MOBILE IDENTIFICATION DEVICES

Effective Date: DD MMM 19
Coordinator: Information Technology Unit

PURPOSE

This order sets forth Department policy and procedure for the use of Mobile Identification Devices (MID). MID allow law enforcement personnel to temporarily cross reference specific biometric data with a handheld device in the field and then wirelessly compare the data to a biometric database for comparison and identification. Identification can be made in near real time without having to take a subject to a detention facility for the identification process.

A. DEFINITIONS

A - 1. Authorized User

A member trained in the use of the MID and accompanying software. Only authorized users may use the MID.

A - 2. Mobile Identification Devices (MID) Currently Used by the Department

As of the effective date of this order, the Department uses wireless Bluetooth-enabled fingerprint scanners which pair with software on a Mobile Data Terminal (MDT) to compare fingerprints obtained from a person with fingerprints in the CAFIS fingerprint database.

A - 3. Cogent Automated Fingerprint Identification System (CAFIS)

A regional fingerprint database shared by Alameda and Contra Costa Counties.

B. DESCRIPTION OF THE TECHNOLOGY

B - 1. The MID System

Mobile Identification Devices (MID) are handheld devices with an optical sensor that scans fingerprints and match them with fingerprint databases. The MID uses the Bluetooth wireless radio standard to send a scanned image of a fingerprint to a police vehicle mobile data terminal (MDT) with special software. The software accesses a regional fingerprint database shared by Alameda and Contra Costa Sheriff's Offices – Cogent Automated Fingerprint Identification System (CAFIS).

B - 2. How MID Works

The MDT software sends the fingerprint digital image to CAFIS where the Almeda and Contra County CAL-ID Mobile Web ID system runs the fingerprint against the CAFIS system to look for matches; the software match

process uses a graphic representation of the print as a mathematical model of the relationships between the ridges of the fingerprint image. This mathematical measuring of ridge lines allows the image to be transmitted as a string of numbers the Automated Fingerprint Identification System (AFIS) databases can use.

Search results are sent back to MDTs. If a search result ends with a 'hit' to a fingerprint record in CAFIS, a return with limited data (Transaction number (of the search), name on record, date of birth (DOB), Sex, Person File Number (PFN)/Juvenile File Number (JFN) and booking photo (if there is a previous arrest booking number) will be displayed. The hit will only return with the record hit (not a list of possible matches). No hits return with the display, "No hit."

C. AUTHORIZED USE POLICY

C - 1. Identification of Detained and Arrested Subjects

Prior to using MID, members shall use available databases (e.g. CRIMS, DMV, CalPhoto) as the primary means of identifying persons. If available databases are not sufficient to positively identify a subject who must be identified on scene, the MID may be used to identify the subject. A MID may only be used when the individual provides knowing and voluntary[1] consent (captured via Body-Worn Camera (BWC) video or on a signed consent form[2], and one of the following circumstances exist:

1. Probable causes exists for the subject's arrest; or
2. The subject is to be cited for an infraction or misdemeanor and cannot provide satisfactory evidence of identity.

C - 2. Assistance to Other Agencies

Providing MID assistance to other agencies shall be approved by a supervisor or command officer. All instances of such outside assistance shall be documented, at minimum, by a notation on the Computer-Aided Dispatch (CAD) incident. Mobile identification assistance provided to other law enforcement agencies must be carried out in accordance with all sections of this use policy including section D "Prohibited Uses and Actions," Section D "Data Collection, Access, Protection, Retention, Sharing, and Maintenance," and Section F "Data Collection, Access, Protection, Retention, Sharing, and Maintenance."

C - 3. Other Uses of MID

[1] Officers seeking consent shall tell the subject that they have the right to refuse being identified via MID.

[2] As of the effective date of this order, the form number is TF-2018.

Any use of the MID for reasons other than set forth in B-1 and B-2 shall be approved by a supervisor or command officer prior to use.

C - 4. Documentation of MID Use

All instances of MID use, other than training, shall be documented in the appropriate report (or CAD incident for outside agency assistance). Documentation shall include the basis for use of the MID and, if directed by a supervisor or commander, the name and serial number of that member.

D. PROHIBITED USES AND ACTIONS

D - 1. Tampering with or Modifying the MID

Members shall not tamper with or modify the MID. All loss or damage of MID shall be reported in accordance with DGO N-05, *Lost, Stolen, Damaged City Property*, with a copy of the memo routed to the Information Technology Unit.

D - 2. General Investigative Purposes or Intelligence Gathering

MID shall not be used for general investigative purposes or intelligence gathering absent an authorized use as prescribed in section B.

D - 3. Physical Force or Coercion

Members shall not use physical force or coercion to force a subject to submit to use of an MID.

E. DATA COLLECTION, ACCESS, PROTECTION, RETENTION, SHARING, AND MAINTENANCE

E - 1. Data Collection

The MID operate by collecting specific fingerprint data through electronic scanning technology.

E - 2. Data Access

The Alameda County Sheriff's Office (ACSO) Central Identification Bureau (CIB) maintains all data access. MID user access is limited to the results of a fingerprint search through the Mobile WEB ID system.

Public and defendant access to the database shall follow the same rules as currently established for public access to CAFIS.

E - 3. Data Protection

Data is transmitted from the MID to the MDT by secure Bluetooth connection, and then from the MDT to the CAFIS database and back via encrypted wireless connection.

E - 4. Data Retention

The MID will hold up to 10 searches (in case out of range of the MDT) until they are 'sent' to search against the Alameda /Contra Costa fingerprint database. ACSO CIB logs and maintains transaction information. Data is purged from the MID after being sent to the MDT; data is not stored in the MDT.

F. TECHNOLOGY ADMINISTRATION

F - 1. Third-Party Data Sharing

OPD assistance to outside agencies is governed by B-2. Outside agencies requesting MID use shall be responsible for possessing the appropriate basis for requesting the data.

F - 2. Data and Equipment Maintenance

ACSO's CIB manages Alameda County's CAL-ID System infrastructure consisting of an infrastructure of CAL-ID systems, sub-systems and network. The main CAL-ID system is an Automated Fingerprint Identification System (AFIS). CAL-ID includes several supporting systems also referred to as 'sub-systems' that provide additional information and tools to law enforcement. Supporting systems include mugshot and mobile ID systems. Management includes all CAL-ID databases, equipment, system and equipment maintenance, equipment deployment, training and system access.

Alameda County Mobile ID devices use the CAL-ID Mobile WEB ID system to run fingerprint searches against the fingerprint database. MID users must log into the Mobile ID WEB ID systems to use the Mobile ID device and receive search results. Only the Alameda/Contra Costa County fingerprint database is searched.

All mobile ID results return to laptops in the patrol vehicles (MDT). If a search results ends with a 'hit' to a fingerprint record in the Alameda/Contra Costa County database, a return with limited data [Transaction number, Name on record, DOB, Sex, Person File Number (PFN)/Juvenile File Number (JFN) and booking photo] will be displayed. The hit will only return with the record hit (not a list of possible matches).

F - 3. Training

All users must first complete the Mobile ID User Agreement and receive hands-on training. The agreement is signed by their supervisor and sent to ACSO's CIB for final approval and user account access. When the user signs the Mobile Identification User Agreement, they certify that they have read and

will comply with the Mobile Identification Policy, have received all required training documents, and will abide by all policies.

Any maintenance required of the MID will done by ACSO staff, and requests will be directed to ACSO through the OPD ITU.

By order of

Anne E. Kirkpatrick

Chief of Police Date Signed: _____

Last Updated 2019.11.30

Alternate Resolution Language

WHEREAS, the City of Oakland has a strong tradition of embracing and valuing diversity and respecting the civil and human rights of all residents regardless of race, religion, political opinion, or national origin; and

WHEREAS, the City Council acknowledges that cities across the country, including San Francisco[1], Portland[2], Albuquerque, Saint Paul, and Atlanta have ended their participation in various federal task forces, including the Federal Bureau of Investigation's (FBI) Joint Terrorism Task Force (JTTF) because of the federal government's refusal to allow local police departments to follow state and local laws; and

WHEREAS, the City Council finds that the FBI and the JTTF has a troubling history of profiling individuals and communities based on their race, religion, national origin, and political opinion; and

WHEREAS, in its April 1, 2010-September 30, 2010 "Semiannual Report to Congress", the Office of the Inspector General found that the FBI's "factual basis for opening some of the investigations of individuals affiliated with the groups was factually weak, and in several cases there was little indication of any possible federal crimes"; that the FBI "extended the duration of investigations involving advocacy groups or their members without adequate basis, and in a few instances the FBI improperly retained information about the groups in its files"; that the FBI also "classified some investigations relating to nonviolent civil disobedience under its "Acts of Terrorism" classification, which resulted in the watch listing of subjects during the investigation"; that the FBI "inappropriately used a confidential informant to collect and retain information about the First Amendment expressions of persons associated with the Pittsburgh Organizing Group"; that the FBI's initiating of a case pertaining to an individual associated with PETA "did not support opening any investigation at all"'; that the FBI "opened investigations of individuals associated with Greenpeace based on concerns about potential illegal conduct, such as trespass, and vandalism"; that the FBI's files "contained information about nonviolent civil disobedience by Catholic Worker members "peaceful trespass on a military facility"[3]; and

WHEREAS, the City Council finds that after the tragic events of 9/11, the FBI used bogus counterterrorism measures to entrap an innocent California man and wrongfully prosecute and imprison him for 14 years on terrorism charges based solely on his religious views and national origin;[4] and

WHEREAS, Oakland has been on record as a City of Refuge since July 8, 1986; and

WHEREAS, on July 18, 2017, the Oakland City Council unanimously passed Resolution No. 86860, which directed the City Administrator to immediately terminate a cooperation agreement between the Oakland Police Department (OPD) and Immigration and Customs Enforcement (ICE), this directive was ignored, and OPD participated in an ICE raid in West Oakland on August 16, 2017[5]; and

---

[1] https://sanfrancisco.cbslocal.com/2017/02/01/san-francisco-police-department-suspends-participation-with-fbi-joint-terrorism-task-force/

[2] https://www.wweek.com/news/city/2019/02/13/portland-leaves-the-joint-terrorism-task-force-again-becoming-second-city-to-cut-ties/

[3] https://oig.justice.gov/semiannual/1011/fbi.htm

[4] https://www.ocregister.com/2019/08/16/lodi-terror-case-shows-injustice-results-when-fear-rules/

[5] https://www.eastbayexpress.com/SevenDays/archives/2017/10/12/oakland-city-council-to-hold-hearing-on-controversial-ice-raid-and-oakland-police-misinformation

WHEREAS, ICE is the second largest member of the JTTF by number of agents; and

WHEREAS, the FBI and the JTTF actively worked with ICE to deport a Texas man with DACA status, because of his political views;[6] and

WHEREAS, the "FBI is monitoring groups on the border that are protesting U.S. immigration policy"[7]; and

WHEREAS, the City Council finds that the San Francisco office of the FBI, which runs the Bay Area Joint Terrorism Task Force that the OPD is part of, investigated California civil rights groups as terrorism threats;[8] and

WHEREAS, "members of an FBI Joint Terrorism Task Force tracked the time and location of a Black Lives Matter protest" at the Mall of America in Bloomington, Minnesota after a tipster contacted the FBI and said some vandalism may occur. No mention of potential vandalism is present in the JTTF email chain, and no vandalism or any acts of violence occurred at the protest[9]; and

WHEREAS, "the FBI is investigating political activists campaigning against the Dakota Access pipeline, diverting agents charged with preventing terrorist attacks to instead focus their attention on indigenous activists and environmentalists[10]; and

WHEREAS, the FBI's 2018-2019 "Threat Guidance" stated that Black Identity Extremists and Animal Rights/Environmental extremists were the top existential threats[11]; and

WHEREAS, the mission of the OPD is to protect the safety of the public against crimes committed by persons in accordance with the laws of the State of California and the City of Oakland, and the policies of the Police Department; and

WHEREAS, the City of Oakland has previously entered into a Safe Streets Task Force agreement with the FBI to combat violent crimes, which states that its mission "is to identify and target for prosecution criminal enterprise groups and individuals responsible for crimes of violence such as murder and aggravated assault, bank robbery, Hobbs Act offenses, extortion, transportation crimes, special jurisdiction matters, and other violent incident crimes, as well as to focus on the apprehension of dangerous fugitives where there is or may be a federal investigative interest; and

WHEREAS, on June 2, 2015, the City Council voted to authorize the "FBI buildout" at OPD headquarters and to amend the Safe Streets Task Force agreement to restrict FBI involvement to homicide investigations only, and this restriction was ignored, and no amendment occurred; and

WHEREAS, the City Council finds that the FBI has actively resisted and worked to thwart local efforts at transparency and accountability and worked with local police departments to mislead elected officials and the public about the scope of joint terrorism investigations in the Bay Area;[12] and

---

[6] https://theintercept.com/2019/11/02/deportation-occupy-ice-daca/
[7] https://news.yahoo.com/exclusive-document-reveals-the-fbi-is-tracking-border-protest-groups-as-extremist-organizations-170050594.html
[8] https://www.theguardian.com/us-news/2019/feb/01/sacramento-rally-fbi-kkk-domestic-terrorism-california
[9] https://theintercept.com/2015/03/12/fbi-appeared-use-informant-track-black-lives-matter-protest/
[10] https://www.theguardian.com/us-news/2017/feb/10/standing-rock-fbi-investigation-dakota-access
[11] https://www.newsweek.com/fbi-leak-black-identity-extremist-threat-1453362
[12] https://theintercept.com/2019/11/01/fbi-joint-terrorism-san-francisco-civil-rights/

WHEREAS, on June 8, 2012, the City of San Francisco enacted Ordinance No. 2A.74 et seq., the "Safe San Francisco Civil Rights Ordinance", which states in relevant part that the San Francisco Police Department may only assist the JTTF in a manner that is fully consistent with the laws of the State of California, as well as the laws and policies of the City of San Francisco, including but not limited to Police Department policies, procedures, and orders; and

WHEREAS, in December 2016, the FBI produced a white paper which essentially concluded that San Francisco could only comply with its "Civil Rights Ordinance" if San Francisco's standing orders, policies, or ordinance were weakened, only sanitized information was provided in the required annual report, San Francisco withdraws from the JTTF, or its task force officers are not assigned any investigations or leads[13]; and

WHEREAS, on October 3, 2017, the City Council enacted Ordinance No. 13457 C.M.S., Chapter 9.72 et seq., which states in relevant part that the Oakland Police Department may only assist the JTTF in a manner that is fully consistent with the laws of the State of California, as well as the laws and policies of the City of Oakland, including but not limited to Police Department policies, procedures, and orders; and

WHEREAS, the FBI JTTF Memorandum of Understanding (MOU) states that "JTTF personnel are not permitted to discuss official JTTF business with supervisors who are not members of the JTTF unless the supervisor possesses the appropriate security clearance and the dissemination or discussion is specifically approved by the FBI JTTF Supervisor[14]", which could prohibit OPD's compliance with Oakland's "Transparency and Accountability for City Participation in Federal Surveillance Operations" Ordinance No. 13457 C.M.S., Chapter 9.72.010; and

WHEREAS, under the Oakland City Charter section 504(l) (Charter section 504(l)), any interagency agreement between the City and another public agency for joint governmental actions, such as a "Memorandum of Understanding" (MOU), must be approved by the City Council and the public has a right to speak on the items; and

WHEREAS, the "Transparency and Accountability for City Participation in Federal Surveillance Operations" Ordinance No. 13457 C.M.S., Chapter 9.72.010 requires that before execution of any MOU between OPD and the FBI, the Chief of Police shall submit the proposed MOU and any orders, policies, and procedures relevant to the subject matter of the MOU for discussion and public comment at an open meeting of the Privacy Advisory Commission; and

WHEREAS, by participating in the JTTF since at least 2007 without City Council approval, OPD has been in continuous violation of Oakland City Charter Section 504(l); and

WHEREAS, the FBI and JTTF may conduct surveillance without reasonable suspicion, in conflict with state law (Cal. Const. Article 1, Section 1, *White v. Davis* (1975) 13 Cal.3d 757), and OPD DGO M-17 Section V A. 1; and

WHEREAS, the FBI and JTTF may conduct demographic mapping, in conflict with state law (SB 31 Religious Freedom Act), Oakland's Sanctuary City ordinance, and OPD DGO M-19 Section III C.; and

WHEREAS, the FBI and JTTF may seize assets pursuant to federal "civil asset forfeiture" guidelines, which conflict with state law (SB 443); and

---

[13] https://www.documentcloud.org/documents/6535344-FBI-White-Paper.html

[14] "Joint Terrorism Task Force Standard Memorandum of Understanding Between the Federal Bureau of Investigation and The Oakland Police Department", Section VI A. 4.

WHEREAS, OPD has deprioritized participation in the JTTF, by assigning one part time employee that "only participated minimally in JTTF operations (approximately 1-2 times a month)"[15] demonstrating a lack of need; and

WHEREAS, the OPD 2018 JTTF annual report states that OPD's JTTF officer was only assigned to assist on one case, that the JTTF officer participated in zero "duty to warn cases", again demonstrating the lack of need; and

WHEREAS, in 2019, OPD informed the Privacy Advisory Commission that the JTTF officer was unaware of the existence of the "Transparency and Accountability for City Participation in Federal Surveillance Operations" Ordinance No. 13457 C.M.S., Chapter 9.72.010, enacted October 3, 2017; now be it

RESOLVED, that pursuant to Ordinance No. 13457, OPD may participate in the JTTF only in a manner that is fully consistent with the laws of the State of California as well as the laws and policies of the City of Oakland, including but not limited to Police Department policies, procedures, and orders; and

FURTHER RESOLVED, that the City Council finds that OPD's participation in the JTTF would violate the "Transparency and Accountability for City Participation in Federal Surveillance Operations" Ordinance No. 13457 C.M.S., Chapter 9.72.010, enacted October 3, 2017, due to existing federal rules and guidelines; and

FURTHER RESOLVED, that OPD shall immediately cease participation in the FBI's JTTF, and shall immediately destroy any files or information retained pursuant to JTTF investigations, unless federal or state law requires their retention.

[15] Draft "OPD FBI 2018 Joint Terrorism Taskforce (JTTF) Annual Report", dated June 28, 2019

BRENNAN CENTER FOR JUSTICE TWENTY YEARS

Brennan Center for Justice
at New York University School of Law

120 Broadway, Suite 1750
New York, NY 10271
646.292.8310 Fax 212.463.7308
www.brennancenter.org

Testimony of Michael German, Fellow,
Brennan Center for Justice at New York University School of Law,
Liberty and National Security Program;
Former Special Agent, Federal Bureau of Investigation

Before the
Portland City Council
April 18, 2018

Mayor Wheeler and Council Members,

It is my pleasure today to testify on behalf of the Brennan Center for Justice's Liberty and National Security Program. We believe that national security policies and practices are most effective when they respect constitutional values and the rule of law, are subjected to stringent oversight, and public accountability. My 16 years as an FBI special agent taught me this was true. I worked undercover on domestic terrorism investigations overseen by Joint Terrorism Task Forces (JTTF) in Los Angeles and Seattle in the 1990s. In those cases, I operated under Attorney General's Guidelines that required me to have a reasonable indication that each person I investigated was engaging in or likely to engage in a violation of federal law. This standard was essentially the same as that imposed by Oregon's criminal intelligence statute.[1] Both were enacted for the same purpose: to protect the privacy and civil liberties of innocent persons and ensure law enforcement activities are based on evidence of wrongdoing rather than bias. As a working agent, I also found this reasonable standard made my investigations more effective, by focusing my efforts and resources where the evidence directed.

Unfortunately, after the 9/11 attacks, the Justice Department and Congress altered the FBI's authorities significantly, giving it power to conduct electronic surveillance, gather intelligence, and investigate people and organizations it does not suspect of engaging in criminal activity. As a result, Portland police officers assigned to the JTTF would find it extremely difficult, if not impossible to comply with Oregon law while conducting routine operations under the FBI's current counterterrorism authorities and practices. Moreover, the FBI exercises these expanded powers in nearly complete secrecy, giving overseers, the public, and victims of abuse few opportunities to challenge them for legality or effectiveness.

Congress passed the USA PATRIOT Act weeks after the attacks, easing the use of secret foreign intelligence powers to amass enormous databases containing information about persons two and three degrees separated from individuals who are merely "relevant" to an authorized inquiry.[2]

Congress continued reauthorizing its most problematic provisions even after Justice Department Inspector General audits began revealing widespread abuse in 2007, including the use of illegal "exigent letters" to gather telephone toll records of journalists based on faked emergencies.[3] It wasn't until National Security Agency (NSA) whistleblower Edward Snowden provided journalists with documents revealing the government's secret interpretation of the PATRIOT Act that allowed the FBI to gather the phone records of virtually all Americans that even members of Congress realized how expansively the bureau was using these authorities.[4] The FBI also claims the authority to sift through the NSA's vast trove of intercepted international communications without warrants to seek evidence for use in routine criminal investigations against Americans, though it won't say how often it conducts these backdoor searches.[5] Portland police officers assigned to the JTTF have routine access to most of these data bases when conducting counterterrorism investigations or intelligence gathering activities.

The Justice Department also amended the Attorney General's Guidelines that govern the FBI's investigative authorities several times after 9/11, lastly and most significantly by Attorney General Michael Mukasey in December 2008.[6] The Mukasey guidelines created a new type of investigation called an "assessment," and expanded the scope of preliminary investigations, neither of which require reasonable suspicion in order to initiate. Assessments permit physical surveillance, commercial and government database searches, overt and covert interviews, racial and ethnic mapping, and the recruitment and tasking of informants without any factual predicate, that is, without any objective basis to suspect the target of the investigation has violated any law or is likely to in the future.[7]

Agents open assessments by claiming they have an "authorized purpose," like preventing crime or terrorism, but such subjective criteria allow agents immense discretion. Over 82,325 assessments of individuals and organizations that the FBI opened from 2009 to 2011, only 3,315 found information that warranted opening preliminary or full investigations, according to data the FBI released to *The New York Times*.[8] Assessments can be opened for the purpose of finding information to coerce a person to become an FBI informant. Again, no factual predicate suggesting wrongdoing is required.

Preliminary investigations can last up to 18 months and require only "information or an allegation." A 2010 Inspector General inquiry regarding FBI investigations of domestic advocacy groups like the Thomas Merton Center for Peace and Justice, Greenpeace, Catholic Worker, and People for the Ethical Treatment of Animals found FBI agents often make the required allegations, based on the agents' speculation that the subjects might commit a crime in the future.[9] Importantly, though the Inspector General found these investigations problematic, he determined they would be authorized under the Mukasey guidelines. Only full investigations, which allow electronic wiretaps and search warrants, require the reasonable suspicion of criminal activity that Oregon law requires.[10]

The abuse that results from these low standards is not hypothetical. Despite the excessive secrecy shrouding most JTTF activities, substantial public evidence shows the FBI has repeatedly used its post-9/11 powers to harass political dissidents, immigrants, and minority communities. The Portland Police can be proud of the fact they led resistance to this federal overreach when Attorney General Ashcroft ordered FBI agents to conduct "voluntary" interviews of thousands of

Middle Eastern immigrants based on nothing but their national origin. This broad racial and ethnic profiling has not stopped. In 2009 the FBI initiated a nationwide program of mapping American communities by race and ethnicity, and tracking so-called "ethnic behaviors," which the Justice Department specifically authorized in 2014.[11] FBI documents obtained by *The Intercept* reveal agents regularly exploit immigration records, scour Facebook and infiltrate Muslim Students Associations or local mosques to recruit informants.[12] On the eve of the 2016 presidential elections FBI agents conducted at least 109 interviews of American Muslims across the nation, asking generalized questions about potential threats to polling places, and potentially suppressing voter turnout from these communities.[13]

In August 2017, the FBI circulated an intelligence assessment to its local networks, including thousands of local police officers assigned to the JTTF. The document warned of the threat posed to law enforcement by so-called "Black Identity Extremists," a movement it describes as responding to "*perceptions* of police brutality against African Americans."[14] Local law enforcement has adopted this thinly veiled allusion to the Black Lives Matter movement as a threat to be prioritized in investigations.[15] Indeed, the FBI has previously targeted Black Lives Matter activists with intimidating visits to their homes and workplaces, as they have done with environmental activists across the country and here in Portland.[16] These harassing activities do not make us safer.

Portland is the first city to refuse to participate in the JTTF in 2005, but others have now followed this lead. In 2012, the San Francisco City Council passed an ordinance requiring the SFPD to submit annual public reports about its work with the FBI, a process modeled on the Portland ordinance passed in 2011.[17] As in Portland, the JTTF resisted efforts to fully comply with the public reporting requirements. Instead of submitting its report in 2017 as required, the SFPD suspended its participation in the JTTF.[18] Following this action, the Oakland City Council unanimously passed an ordinance requiring that Oakland Police Department officers assigned to the JTTF follow state and local law, submit annual public reports, and obtain approval from the city's Privacy Advisory Committee before signing any Memoranda of Understanding with the FBI JTTF.[19]

These ordinances imposed reasonable and necessary measures to ensure that local police comply with state and local laws and protect their constituents from federal overreach and abuse. JTTF officials' failure to fully comply with them reveals such measures are insufficient, however. By withdrawing from the JTTF, the City of Portland would rejoin the frontlines of a movement to uphold the constitutional rights of its constituents and hold federal agencies accountable to the law. Ensuing public safety includes protecting against unwarranted government interference with the free exercise of our civil rights and liberties.

---

[1] Or. Rev. Stat. § 181A.250, https://www.oregonlegislature.gov/bills_laws/ors/ors181a.html.

[2] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 107 P.L. 56, 115 Stat. 272.

[3] OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS (2010), available at http://www.justice.gov/oig/special/s1001r.pdf
[4] Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian,* June 5, 2013, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order.
[5] Louise Matsakis, "Congress Renews Warrantless Surveillance – And Makes It Even Worse," *Wired Magazine*, Jan. 11, 2018, at: https://www.wired.com/story/fisa-section-702-renewal-congress/.
[6] See Emily Berman, "Domestic Intelligence: New Powers, New Risks," *Brennan Center for Justice at New York University Law School*, January 18, 2011, https://www.brennancenter.org/publication/domestic-intelligence-new-powers-new-risks.
[7] U.S. Department of Justice, Office of the Attorney General, *The Attorney General's Guidelines for Domestic FBI Operations* (2008), https://www.justice.gov/archive/opa/docs/guidelines.pdf.
[8] Charlie Savage, "F.B.I. Focusing on Security Over Ordinary Crime," *The New York Times*, August 23, 2011, sec. U.S., https://www.nytimes.com/2011/08/24/us/24fbi.html.
[9] OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S INVESTIGATIONS OF CERTAIN DOMESTIC ADVOCACY GROUPS (2010), http://www.justice.gov/oig/special/s1009r.pdf
[10] Or. Rev. Stat. § 181A.250.
[11] The Department of Justice, *Guidance for Federal Law Enforcement Regarding Their Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation*, December 2014, https://www.justice.gov/sites/default/files/ag/pages/attachments/2014/12/08/use-of-race-policy.pdf. See also, Federal Bureau of Investigation, *Domestic Investigations and Operations Guide (DIOG)*, December 16, 2008.
[12] Cora Currier, "The FBI Wanted to Target Yemenis Through Student Groups and Mosques," *The Intercept*, September 29, 2016, https://theintercept.com/2016/09/29/the-fbi-wanted-to-target-yemenis-through-student-groups-and-mosques/; and Cora Currier, "Revealed: The FBI's Secret Methods for Recruiting Informants at the Border," *The Intercept*, Oct. 5, 2016, https://theintercept.com/2016/10/05/fbi-secret-methods-for-recruiting-informants-at-the-border/
[13] Mazin Sidahmed, "FBI Pre-election Sweep of Muslim Americans Raises Surveillance Fears," *The Guardian*, Jan. 16, 2017, https://www.theguardian.com/us-news/2017/jan/16/fbi-muslim-americans-visits-surveillance-cair.
[14] Jana Winter and Sharon Weinberger, "The FBI's New U.S. Terrorist Threat: 'Black Identity Extremists,'" *Foreign Policy*, October 6, 2017, https://foreignpolicy.com/2017/10/06/the-fbi-has-identified-a-new-domestic-terrorist-threat-and-its-black-identity-extremists/.
[15] Martin De Bourmont, "Is a Court Case in Texas the First Prosecution of a 'Black Identity Extremist'?," *Foreign Policy*, January 30, 2018, https://foreignpolicy.com/2018/01/30/is-a-court-case-in-texas-the-first-prosecution-of-a-black-identity-extremist/; Will Parrish, "Documents: Police Targeted Leftists Before 'Unite The Right' Rally," Shadowproof, March 7, 2018, https://shadowproof.com/2018/03/07/documents-reveal-police-targeting-anti-racists-charlottesville/.
[16] Adam Federman, "Lawyer for Environmental Group 'interrogated Repeatedly' at US Border," the Guardian, July 6, 2015, http://www.theguardian.com/us-news/2015/jul/06/environmental-group-lawyer-interrogated.
[17] San Francisco, Calif., Admin. Code § 2A.74 (2012); Brandon E. Patterson, "Are Police Targeting Black Lives Matter Activists Ahead of the GOP Convention?", Mother Jones, June 30, 2016, https://www.motherjones.com/politics/2016/06/cleveland-protesters-rnc-police-fbi-visits/
[18] "SFPD Suspends Participation with the Joint Terrorism Task Force," news release, February 1, 2017, http://sanfranciscopolice.org/article/sfpd-suspends-participation-joint-terrorism-task-force.
[19] Oakland, Calif., City Council Ord. 13457, § 2 (October 3, 2017), https://library.municode.com/ca/oakland/codes/code_of_ordinances?nodeId=TIT9PUPEMOWE.