DEPARTMENTAL GENERAL ORDER

Attachment A

I-21: MOBILE IDENTIFICATION DEVICES

Effective Date: DD MMM 19
Coordinator: Information Technology Unit; Bureau of Field Operations Division (BFO)

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. Use Procedure

MID devices will be stored with BFO; patrol officers requesting to use a MID shall contact their supervising sergeant. The sergeant will direct the officer to retrieve the MID from BFO offices or to have another personnel member deliver the MID in the field for identification purposes.

C - 3. 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

[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.

"Data Collection, Access, Protection, Retention, Sharing, and Maintenance," and Section F "Data

C - 4. Other Uses of MID

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 - 5. 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 / 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. Public Access

Requests for MID data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public Records Access (Civil Code § 1798.90.55).

E - 4. 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 - 5. 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. System Coordinator / Administrator

The OPD Information Technology Unit (ITU) shall administer the MID program. ITU shall be responsible for collaborating with the Training Division to ensure that personnel with access to the system are properly trained. ITU or other designated personnel shall also be responsible for any required audits in support of the annual report to the City's Privacy Advisory Commission and City Council.

F - 2. Maintenance

ITU will also collaborate as necessary with ACSO / CIB to maintain system operations.

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 - 3. 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 - 4. 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.
Any maintenance required of the MID will done by ACSO staff, and requests will be directed to ACSO through the OPD ITU.

F - 5. Auditing and Oversight

The System Coordinator will be responsible for coordinating audits every year to assess system use. The System Coordinator will collaborate with ACSO to produce a report detailing use of each device. A summary of user access and use will be made part of an annual report to the City's Privacy Advisory Commission and City Council.

By order of

Anne E. Kirkpatrick
Chief of Police

Date Signed: _____