

# Mobile Identification Technology

## 449.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of Mobile Identification Technology. The mobile identification device (MID) is intended for use by an officer in the field to assist in the rapid identification of a person. The goal of the system includes: minimize the duration of detentions, decrease misidentification, identify wanted persons, identify missing or incapacitated persons, and reduce the time needed to verify a person's identity.

## 449.2 POLICY

This policy provides guidelines for the issuance and use of the MID. Only members who have received Department-approved training in the MID shall access or operate a MID. Training includes review of this policy, the proper handling of Criminal Offender Record Information (CORI) and the operation and care of MID units. Additionally, a MID shall only be used in circumstances where a Department member has the legal right to obtain or request identification from a subject for criminal justice purposes.

Reasonable attempts must first be made to obtain a person's identifying information. Mobile Identification Technology may not be used as a substitute for identifying persons when other forms of valid identification are readily available.

Mobile Identification Technology may only be installed on Department owned and operated devices which meet Cal DOJ requirements.

~~Mobile ID—A handheld combination of hardware device(s) and software used to capture biometric information for transmission and comparison to law enforcement databases.~~

~~Fingerprint scanner—The portion of the Mobile ID system which captures an electronic representation of a person's fingerprint.~~

~~Mobile Identification Technology—A computerized system that utilizes Mobile ID units to capture biometric information from persons in the field. The information is electronically transmitted to Automated Fingerprint Identification System ( AFIS ) and the FBI 's Repository for Individuals of Special Concern (RISC) for analysis.~~

## 449.3 DEFINITIONS

Mobile Identification Device (MID) – A handheld combination of hardware device(s) and software used to capture biometric information for transmission and comparison to law enforcement databases.

# Bay Area Rapid Transit Police Department

## BART PD Policy Manual

### *Mobile Identification Technology*

---

Mobile Identification Technology – A computerized system that utilizes MID units to capture biometric information from persons in the field. The information is electronically transmitted to California's Department of Justice's (DOJ) Automated Fingerprint Identification System (AFIS) and the Federal Bureau of Investigation's (FBI)'s Repository for Individuals of Special Concern (RISC) for analysis.

Fingerprint scanner – The portion of the MID system which captures an electronic representation of a person's fingerprint.

#### **449.4 DESCRIPTION AND BACKGROUND**

The DOJ MID system was developed to provide rapid identification in the field. The fingerprint images are captured utilizing an authorized handheld mobile identification device and are searched against fingerprint images that reside in AFIS and RISC. The MID search and response information is construed as CORI. Therefore, all CORI statutes, rules, and policies apply regarding access to data, including California law and regulations, the California Law Enforcement Telecommunication System (CLETS) Policies, Practices, and Procedures, the FBI Criminal Justice Information Services (CJIS) Security Policy, and federal regulations. MID users will follow the guidelines set forth in the California Penal Code

The MID unit is a palm-sized device that scans a subject's fingerprints and sent via a wireless connection to search against the AFIS or RISC. If the subject's fingerprints have previously been entered into the AFIS or RISC database, the subject's archived data will return with positive matches in the system. For any returns on subject's matching, officers are prohibited from relying solely on the AFIS and RISC search responses as the impetus for any law enforcement action.

Biometric information captured by MID shall not be stored beyond the time needed to process each transaction

#### **449.5 DEPLOYMENT AND USAGE**

Officers authorized to use the MID will have their own individual login information and shall not share login credentials with others.

At no time will an officer capture fingerprints for a MID search outside their official law enforcement duties. Information gathered is on a "need to know" basis. MID shall not be used for random or general investigative or intelligence gathering. MID may be used during a legal detention, arrest, or criminal investigation in the following circumstances:

- The person does not possess or is unwilling to provide valid identification.

# Bay Area Rapid Transit Police Department

## BART PD Policy Manual

### *Mobile Identification Technology*

---

- There is doubt of the authenticity of any identification that is presented.
- The person provided a name and date of birth in which officer discovers is not accurate.
- A person is driving a motor vehicle and does not possess a valid driver's license.

During a consensual contact, officers will not take the person's fingerprint without the person's consent. If at any time the person withdraws consent, the officer must stop the fingerprint process.

The identification information provided using MID is considered to be supplemental information and shall be used to compare, evaluate, and/or corroborate information obtained through other investigative methods. MID shall not be used as a sole criteria for confirming a person's identity.

MID data is only an aid to identify a person and shall not be used as the sole grounds for establishing probable cause for arrest.

#### **449.6 PROCEDURE**

Use of a MID will often require an officer to use both hands to operate the device while also diverting their attention away from the person they are trying to identify. An officer should employ good safety measures before using MID such as: presence of additional officers, placing the subject in a position of disadvantage or if warranted, handcuffing the subject.

For fingerprint samples, a left or right slap of prints is captured (includes index and middle finger).

The MID will indicate the quality of the image. If quality is low, another attempt should be made, or other fingers should be selected.

Information requests submitted through a MID will result in one of three responses:

- HIT – There is a high probability the record returned matches the sample submitted. The name, date of birth, and possibly the CII number, and FBI number.
- PROBABLE HIT – The record returned likely matches the sample submitted but additional follow-up will be needed. The name, date of birth, and possibly the CII number, and FBI number.
- NO HIT – No match was made. This response simply means no record was found. This could indicate no biometric data for the person was ever submitted to Cal DOJ or the sample was of poor quality.

Any relevant information obtained from the response may be relayed to Dispatch in order to request appropriate record checks.

# Bay Area Rapid Transit Police Department

## BART PD Policy Manual

### *Mobile Identification Technology*

---

[A notation should be made in the CAD detail stating MID was used.](#)

#### **449.7 UNAUTHORIZED USE**

[Any unauthorized use of the MID may result in:](#)

- [Removal of MID user privileges.](#)
- [Progressive disciplinary action up to and including termination.](#)

#### **449.8 REPORTING OF DAMAGE**

Any employee who discovers a MID ~~Mobile-ID~~ unit damaged or missing shall report their finding to their supervisor. The supervisor receiving the report will be responsible for providing a description of the damage and a request for a replacement to their assigned Commander or Lieutenant, copying the Operations Deputy Chief, the Civilian Supervisor of Property, and the Police Technology Administrator.