ST. PETERSBURG POLICE DEPARTMENT	DATE OF ISSUE	EFFECTIVE DATE	NUMBER
GENERAL ORDER	March 2019	Immediately	**III-33**
	Distribution: All Employees		

Subject: **MOBILE FINGERPRINT DEVICE**

Index as:
- Ambiguous Response
- Biometric Identification Technology
- Biometrics
- Fingerprints
- Hit Response
- Mobile Fingerprint Device
- No Hit Response
- Statewide Criminal History
- State ID Number

Accreditation Standards: 42.2.2
Cross Reference:
Replaces: Chief's Memo 19-001. III-33 Mobile Fingerprint Device (January 7, 2019)

This Order establishes guidelines and procedures for using biometric identification technology through the use of a Mobile Fingerprint Device. It consists of:

I. Purpose
II. Definitions
III. Procedures

I. PURPOSE

A. The purpose of this Order is to establish guidelines and procedures of the use and deployment of Mobile Fingerprint Device to identify individuals who are unable or reluctant to properly identify themselves and to assist Officers with on-scene identification of individuals.

B. The use of the Mobile Fingerprint Device is intended to provide authorized personnel with a specialized tool to assist in the positive identification of individuals under the appropriate circumstances.

II. DEFINITIONS

A. Biometrics – Distinctive and measurable human characteristics that can be used to identify people apart from demographic data like name and date of birth. Fingerprints and facial features are examples of commonly used biometrics. Since biometrics are unique to individuals, they are more reliable in verifying identity than knowledge-based methods.

B. Hit Response – A "match" was found in the FDLE database of criminal records for the fingerprints submitted and the FDLE number is returned.

C. No Hit Response – No match was found in the FDLE database of criminal records.

D. Ambiguous Response – There was no definitive match using the submitted search points. More than one possible match was found.

E. Mobile Fingerprint Device – A fingerprint identification system that uses two fingers to search state wide criminal history records and return positive identification along with criminal history information on an individual.

F. State ID Number (also known as FDLE number) – The sequential number assigned to an individual's record by the Florida Department of Law Enforcement (FDLE) which allows retrieval of an individual's complete, statewide criminal record.

G. Statewide Criminal History – A listing of an individual's arrests, prosecutions, demographic data used by that individual in the criminal justice system, and a "flag" when a DNA sample is on file for that individual.

III. PROCEDURE

A. The Mobile Fingerprint Device will only be used by those authorized personnel that have had the training and demonstrated proficiency in the operation of the unit.

1. Training shall include considerations and requirements for the use of the device under various circumstances.

2. Personnel must hold a current active CJIS certification to participate in the training and deployment of the Mobile Fingerprint Device.

3. Training will include at a minimum:
   a. Setup and maintenance procedures;
   b. Proper use guidelines;
   c. Legal issues involved in the use of the Mobile Fingerprint Device; and
   d. Reporting requirements.

B. All Mobile Fingerprint Device units and components shall be approved, inspected, and installed as determined by the ITS division.

C. Guidelines for the use of the Mobile Fingerprint Device

1. Consent:

a. The Mobile Fingerprint Device may be used in situations where the subject to be fingerprinted has given a knowing and willing voluntary consent or the permission for the Officer to use the device.

b. This may include consent given during lawful encounters (i.e. consensual encounters, traffic stops, and investigative detentions).

1) As with other forms of consent, the consent can be limited or withdrawn at any point by the subject.

2) If consent is withdrawn, use of the Mobile Fingerprint Device is not authorized and its use must stop immediately.

3) Authorized users shall not force or coerce anyone to submit to the scan.

4) If an incident report is taken, the Officer shall document that the subject provided consent for the use of the Mobile Fingerprint Device.

5) If an incident report is not taken, the Officer shall notate in the call notes that the subject provided consent for the use of the Mobile Fingerprint Device.

2. Reasonable Suspicion

a. The Mobile Fingerprint Device may be used in situations where reasonable suspicion can be articulated, to include, but not limited to:

1) The subject to be printed has committed or is about to commit a criminal act.

2) When there is a justifiable and reasonable belief that such printing via the Mobile Fingerprint Device will either help establish probable cause or dispel the Officer's reasonable suspicion. In this instance, the Mobile Fingerprint Device should be used as quickly as possible after the Officer establishes reasonable suspicion that the subject is or was involved in a criminal act.

3) The Mobile Fingerprint Device shall not be the first investigative tool used, when attempting to identify a subject under reasonable suspicion. The Officer shall utilize other investigative means prior to the use of the Mobile Fingerprint Device These may include, but are not limited to:

a) Interviewing the subject,
b) Attempting to identify the subject through authorized databases,
c) Identification through photo ID, or
d) Gaining consent for use of the Mobile Fingerprint Device from the subject.

3. Probable Cause

a. The Mobile Fingerprint Device may be used in situations where the subject to be fingerprinted would otherwise be required to give traditional fingerprint samples, to include but not limited to:

1) Probable cause for a criminal arrest;
2) When a subject is issued a citation that requires fingerprints to be affixed, the Mobile Fingerprint Device may be used to rapidly confirm the identity of the subject;
3) Where a court order requiring the use has been rendered.

4. Non-Standard Use

a. Generally, the use of the Mobile Fingerprint Device for random or generalized investigative or intelligence gathering, with no focused case or other reason, is not authorized.

b. Any specialized, non-standard use of the Mobile Fingerprint Device shall require the notification and authorization by an immediate Supervisor.

1) Examples on non-standard use may include the identification of a deceased, unconscious, or otherwise incapacitated subject who cannot be identified by any other means.
2) At the request of an Officer, a Forensic Services Technician may use the Mobile Fingerprint Device to identify a subject.

c. Special care should be taken to ensure the device is not used for improper bias-based profiling.

D. Properly trained personnel may utilize handheld devices for investigations requiring identification or verification of a subject's identity. Fingerprint identification is performed using portable fingerprint capture devices and the dedicated software application on the computer "paired" with the capture device.

1. Search results are returned to both the handheld device and the software application for review.

2. Results are either a "Hit," a "No Hit," or an "Ambiguous" response.

3. In the case of a "No Hit" or "Ambiguous" response, fingers of the subject's other hand may be captured and searched to confirm the original result.

E. All authorized users of the Mobile Fingerprint Device are expected to be able to justify, based upon these guidelines, training, and experience and assessment of the circumstances, how they determined the use of the Mobile Fingerprint Device was justified under the circumstances.

_____
Anthony Holloway
Chief of Police