



University of Pennsylvania Police Department 4040 Chestnut Street, Philadelphia, Pa 19104		 
Directive: 114	Subject: Mobile Fingerprint Identification Scanner (MFID)	Effective Date: 07/30/2020
Order of: Gary Williams, Chief of Police		Amended Date: 08/01/2023

I. Purpose

The purpose of this directive is to define the University of Pennsylvania Police Department's (UPPD's) policy governing the use of the Mobile Fingerprinting Identification Device. This portable device is able to capture an individual's fingerprint and make comparisons in the Pennsylvania AFIS system utilizing the State and Federal database. The device is provided by the Pennsylvania Chiefs of Police Association to securely connect to the PSP AFIS and FBI RISC databases. This device is CJIS compliant.

II. Policy

It is the policy of the University of Pennsylvania Police Department that the use of this device shall be for law enforcement purposes only and done in a manner that is consistent with local, state and federal laws, training and policy. The use of this device is intended to aid in the "on-street" identification of persons that are wanted, persons that appear to be involved in criminal activity, and to accurately identify summary offenders, in the least intrusive manner possible. The use of this device is intended to increase efficiency and enhance the ability to identify individuals during an encounter with law enforcement.

III. Scope

This directive shall affect all sworn police officers.

IV. Definitions

- A. **Mobile Fingerprint Identification Device (MFID)** - A mobile device, which can capture an individual's fingerprint and compare that print against files, contained in the automated fingerprint identification system (AFIS) Multimodal Biometric Identification System (MBIS) databases or the Criminal Justice Information System (CJIS) database. The MFID does not permanently retain any fingerprints captured.

Note: The Pennsylvania Chiefs of Police Association (PCPA) MFID Device will securely connect to the Pennsylvania State Police Automated Fingerprint Identification System (AFIS) and the FBI Repository for Individuals of Special Concern (RISC).

- B. **Device Administrator** – The Captain of Staff and Administrative Services will serve as the device administrator. The Detective assigned as the JNET/TAC/CLEAN Officer for the UPPD will also administrate issues around the use and support of the device.

V. Procedures

A. Authorized User

1. All authorized users will be issued a sign-on code with personal fingerprint identification to activate the MFID. The sign-on allows for an audit trail of persons scanned within the state system. Police personnel that have been authorized and trained to utilize the scanners through the Commonwealth can sign on to any MFID device; the devices are system based and sign-on information is able to be used on any device.
2. In the event a unit is not available or inoperable, an authorized UPPD officers can also utilize an available PPD scanner in the event of similar circumstances.

B. MFID Scanner

1. The MFID charger will be located in the Police Operations Room Supervisors (ORS) Area inside of PennComm. It is recommended to fully charge the scanner and activate only when it is to be utilized for a scan. Turning the scanner 'off' after the scan is completed will help ensure the MFID remains charged throughout the shift.
2. Any device found to be damaged or otherwise malfunctioning shall be removed from service and reported to the ORS and up the chain of command.
3. Damage, loss, or theft of the MFID shall be reported immediately to the on-duty shift supervisor/commander. The reporting officer will prepare a UPPD-10 documenting the nature of the event.
 - a. The on-duty supervisor/commander will notify the Captain of Staff and Administrative Services of the malfunction.

C. USE OF MFID

1. A shift Supervisor/Commander will utilize the appropriate sign-out sheet for the MFID and following physical inspection of the device assign a trained officer to deploy the MFID while on patrol.
2. Only officers who have been trained to operate the MFID will be authorized to perform mobile fingerprinting.

3. The assigned officer is responsible for the security, care and use of the device for the duration of their shift.
4. Police personnel will use the least intrusive method to gain identification, initially attempting to secure 'hard' identification prior to utilizing the MFID; that is, Operators License, Social Security card, work identification, military identification. As with all other UPPD interactions, the officers' Body Worn Camera(s) must be on and recording.
5. The use of J-Net is appropriate prior to utilization of the MFID as another less intrusive option for verification and a photo of the individual.
6. Under no circumstances will an individual be forced to submit to mobile fingerprinting. In the event that an officer is unable to identify an individual where reasonable suspicion exists to warrant such identification, a supervisor shall be notified and will determine the appropriate course of action.
7. Prior to a police officer administering the MFID to an individual, the officer will notify radio of their intent and then will do so ONLY with appropriate back-up personnel present. Due to the proximity to the individual being scanned, and the attention required by the police officer administering the scan, officer safety will be paramount, and scanning will wait until the arrival of sufficient back-up officers.
8. Supervisors should respond to all instances of the MFID being used as available.
9. The finger used to be read by the MFID should make contact 'metal to metal'; that is, flat on the entire reading surface from the bottom metal frame to the top metal frame.
10. There is a photo option on the MFID; authorized users will take a MFID system photograph of the subject prior to scanning to have both identification factors in the system.
11. Documented on the UPPD 10 shall be the following:
 - a. The reason for the stop,
 - b. the use of the MFID,
 - c. the details around the interaction,
 - d. the identity of the officer that completed the scan,
 - e. the reason for doing so (consent, arrest, medical identification), and
 - f. the result of the scan. (The classification of the scan to be noted on all paperwork generated; 'Hit', 'Possible Hit' or 'No Hit'.)
12. All related paperwork shall be completed to include the above information.

13. The mere use of the MFID does not require a 75-48 be taken to the PPD District, however the incident and use of the MFID will be clearly indicated on the UPPD-10 for the incident.

D. Police Interaction and Use of the MFID:

1. **Vehicle Stops**

2. **Summary Offender**- Summary offenders are typically not subjected to fingerprinting, however MFID may be utilized in instances when the individual fails to provide reliable identification.

3. **Medical Emergencies/DOAs**- In cases involving medical emergencies or dead bodies, where there is a need for an immediate identification, MFID may be useful.

- a. MFID should only be used in these cases when other possible means of identification have failed. MFID only searches data from criminal fingerprint files and cannot identify persons that do not have criminal records.
- b. If the MFID is used to identify a person with substantial medical issues, i.e. comatose, the name and contact information of the requesting medical professional will be indicated on the UPPD-10.
- c. If the decedent is suspected to be a victim of violence scanning will not be done until the MFID process is cleared by PPD homicide unit personnel on scene in the ED. The name/badge number of the Homicide Detective authorizing the use of the MFID will be indicated on all UPPD paperwork.

4. The data received will initially be the result of an inquiry against the Federal Megan's Law database, followed by fingerprints residing in the PA State databases. The possibility of Out-of- State records for the person stopped should be consulted through NCIC/PCIC.

E. Care of MFID Device:

1. **Cleaning:** The use of alcohol-based cleaning products is prohibited for any surface of the MFID; a soft cloth, with warm water and soap, can be used to clean the device.

F. Compliance

Violations of this directive, or portions thereof, may result in disciplinary action.

G. Officers Assigned to Other Agencies

Officers of this department assigned to or assisting other law enforcement agencies will be guided by this directive.

H. Application

This directive constitutes departmental policy, and is not intended to enlarge the employer's or employee's civil or criminal liability in any way. It shall not be construed as the creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims insofar as the employer's or employee's legal duty as imposed by law. Violations of policy will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting.