ILLINOIS STATE POLICE DIRECTIVE
OPS-083, MOBILE FINGERPRINT IDENTIFICATION SYSTEM

RESCINDS: OPS-083, 2012-062, revised 08-28-2012	**REVISED:** 10-09-2019 2019-004
RELATED DOCUMENTS: Applicable Department and Division directives and Specialty Manuals	**RELATED CALEA STANDARDS:** 1.2.5

I. POLICY

The Illinois State Police (ISP) will implement and maintain a mobile fingerprint identification system.

II. AUTHORITY

II.A. 20 ILCS 2605/2605-45(4), "Division of Administration"

II.B. 20 ILCS 2605/2605-500(3), "Communication Activities"

II.C. 20 ILCS 2630/0.01 et seq. "Criminal Identification Act"

II.D. 725 ILCS 5/107-14, "Temporary Questioning without Arrest"

III. DEFINITIONS

III.A. Automated Biometric Identification System (ABIS) - the computerized biometric matching system maintained by the ISP that provides automated fingerprint search capabilities and electronic image storage.

III.B. Capture device – a portable fingerprint scanner used to capture and transmit fingerprint images to a mobile data computer.

III.C. Mobile fingerprint image - fingerprint scanned by a capture device.

III.D. Mobile fingerprint identification (Mobile ID) system - portable hardware used to communicate biometric information to ABIS and the Federal Bureau of Investigation's (FBI) Next Generation Identification (NGI) system to identify a person.

III.E. Mobile ID Coordinator – The Illinois State Police, Bureau of Identification (BOI) person assigned to oversee the overall ISP Mobile ID program including user training, system monitoring, and end-user support.,

III.F. Negative response - no personally identifiable information is attached to or associated with the mobile fingerprint image.

III.G. Next Generation Identification System (NGI) – The Federal Bureau of Investigation (FBI) repository of biometric and criminal history information.

III.H. Personally Identifiable Information (PII) - any data that can be used to uniquely identify, contact, or locate a person or entity.

III.I. Positive response – PII is attached to or associated with the mobile fingerprint image.

III.J. Repository of Individuals of Special Concern (RISC) - a limited population of the FBI NGI database including, but not limited to, wanted persons, sex offender registry subjects, and known or suspected terrorists.

III.K. Restricted area - any posted, cordoned off, or otherwise designated area of a building or grounds intended to limit or deny access to a special event of national significance.

IV. PURPOSES FOR COLLECTING MOBILE FINGERPRINTS

IV.A. While following appropriate privacy and civil liberties safeguards to ensure the legal rights of individuals are protected, ISP officers may collect fingerprints to aid in the biometric identification of:

IV.A.1. Individuals who come into direct contact with law enforcement officers during a lawful encounter.

IV.A.2. Individuals who are reasonably suspected of having committed a crime.

IV.A.3. Individuals who a law enforcement officer reasonably suspects are about to commit a crime.

IV.A.4. Individuals who voluntarily request to enter a restricted area.

V. PROCEDURES

V.A. Collection of Mobile Fingerprints

V.A.1. Law enforcement officers may collect, through the use of a Capture Device, fingerprints of individuals with whom they are in personal contact for the purpose of submitting those fingerprints to the ABIS and NGI databases in the following circumstances:

V.A.1.a. With the individual's consent. The consent can be limited or withdrawn by the individual prior to the submission of the mobile fingerprint to the mobile fingerprint ID system. If the fingerprint collection is based solely on consent and the consent is withdrawn in a timely manner, use of the mobile fingerprint ID system must stop immediately;

V.A.1.b. When identifying the individual will help an officer assess the situation and evaluate any threats to the officer's safety or the safety of the community;

V.A.1.c. When state law requires individuals to identify themselves to police officers;

V.A.1.d. When the individual is lawfully detained and using the mobile fingerprint ID system does not prolong the detention beyond the time reasonably required to complete the investigation;

V.A.1.e. When investigating an event involving a fatal or critical injury in which the identity of the deceased/injured is uncertain;

V.A.1.f. Any time a law enforcement officer is permitted or required to take traditional fingerprints of an individual (i.e., the individual is under arrest) (this does not relieve the officer of taking traditional fingerprints);

V.A.1.g. When an officer has made a Criminal History Record Information (CHRI) inquiry using the individual's name, date of birth (DOB) and/or other identifiers and the officer has received responses for multiple individuals with similar identifiers; or

V.A.1.h. When the individual is requesting to enter a restricted area and the individual appears to be age 17 or older.

V.A.1.i. When necessary for training and system testing purposes.

V.B. Guidelines cannot be written to encompass every possible application for the use of a mobile fingerprint ID system. Officers can use the mobile fingerprint ID system in situations other than V.A.1.a. - V.A.1.j., when they can justify the use of the mobile fingerprint ID system, based on these guidelines, training, and experience.

NOTE: ISP personnel may not fingerprint subjects based solely upon their race, ethnicity, citizenship, place of origin, age, disability, gender, sexual orientation, political, religious, or

social views, associations, or the First Amendment protected activities of any individual or any group.

V.C. ISP officers shall not use a mobile fingerprint ID system prior to arrest when the individual presents a valid driver's license or state issued identification card unless:

V.C.1. The officer reasonably suspects the driver's license or identification card is expired, forged, altered, or otherwise fraudulent;

V.C.2. The officer reasonably suspects the individual is presenting, as their own, a driver's license or identification card issued to another person;

V.C.3. The officer has made a CHRI inquiry using the individual's name, DOB, and/or other identifiers, and the officer has received responses for multiple individuals with similar identifiers;

V.C.4. The officer is permitted or required to take traditional fingerprints of the individual (i.e., the individual is under arrest); or

V.C.5. The individual is requesting to enter a restricted area, and the individual appears to be age 17 or older.

V.D. Officers shall not physically force individuals to submit to a fingerprint scan.

VI. DISSEMINATION OF INFORMATION

VI.A. Information received as a result of the use of the mobile fingerprint ID system will be disseminated in accordance with Illinois Administrative Code, Title 20 "Corrections, Criminal Justice, and Law Enforcement," Part 1240 "Law Enforcement Agencies Data System (LEADS)," Section 1240.80 "Dissemination of Data Obtained Through LEADS" and established LEADS policy, procedures, and regulations.

VI.B. When requested by an officer from an outside law enforcement agency to fingerprint a detained individual or a suspect in custody, the requesting officer and agency must comply with this directive and any other applicable department directives and procedures.

VI.C. Officers who are not issued mobile fingerprint ID systems but receive a secondary dissemination of fingerprint responses using Mobile ID Systems are also subject to the terms of this directive.

VII. ACTIONS THAT A LAW ENFORCEMENT OFFICER MAY TAKE BASED UPON MOBILE FINGERPRINT RESULTS

VII.A. ABIS

VII.A.1. Negative Responses – Officers shall take whatever enforcement action they may legally take based upon the circumstances of the encounter.

VII.A.2. Positive Responses – Officers will receive a State Identification Number (SID). Officers may run the SID number through LEADS and take necessary enforcement action based upon the results of the inquiry.

VII.B. NGI

VII.B.1. Negative Responses - Officers will receive a "green" response which indicates there are no candidates for a match in NGI, and officers shall take whatever enforcement action they may legally take based upon the circumstances of the encounter.

VII.B.2. Positive Responses

VII.B.2.a. Red Response = (Highly probable candidate) - There is a high probability that the fingerprint of the individual submitted is among those contained within NGI.

Officers may receive an FBI rap sheet and shall follow the instructions provided in the response. If the officer receives a red response, the officer shall notify the ISP State Terrorism and Intelligence Center (STIC) via e-mail. The e-mail shall contain the reason for the encounter, the disposition, whether there was a positive response from ABIS, and the ISP Computer Aided Dispatch (CAD) number.

VII.B.2.b. Yellow Response = (Possible candidate) - A lower threshold of probability, but still a possibility the individual's PII is in NGI. The officer shall reprint the individual in an effort to gain a higher quality fingerprint and submit the prints again. If the response is yellow a second time, the officer will not reprint the individual, consider the second yellow response as "unable to identify the individual," and take whatever enforcement action they may legally take based upon the circumstances of the encounter.

VIII. RETENTION OF INFORMATION

VIII.A. Capture Device – This device does not store the mobile fingerprint, it is deleted upon being sent to the Mobile Data Computer.

VIII.B. Mobile Data Computer - The PII associated with the mobile fingerprint must be manually deleted from the mobile data computer upon completion of the arrest or incident paperwork.

VIII.C. ABIS Disk Drive - The fingerprint and associated PII, if any, will be retained within the ABIS indefinitely.

VIII.D. Retention of audit and dissemination logs.

The ISP Bureau of Identification (BOI) shall retain its log of all transactions made via the mobile fingerprint ID system pursuant with Section X of this directive.

IX. DATA QUALITY

IX.A. Officers shall inform the BOI in writing if they become aware of any errors in fingerprint identification data.

X. INFORMATION ACCOUNTABILITY

X.A. Any mobile fingerprint ID system submission is logged by ABIS. ABIS transaction audit logs must contain the following information:

X.A.1. The identity of the officer who requested the record;

X.A.2. The date and time the request occurred; and

X.A.3. The positive response information, if any.

X.B. Monitoring system use and conducting audits.

X.B.1. The use of a mobile fingerprint ID system will be monitored and audited in accordance with ISP directives to guard against inappropriate or unauthorized use.

X.B.2. The ISP shall:

X.B.2.a. Certify that each officer using the mobile fingerprint ID system has been trained in accordance with this directive; and

X.B.2.b. Limit the issuance of a mobile fingerprint ID system to officers who have been trained in its use.

XI. TRAINING

XI.A. The ISP will train each officer using a mobile fingerprint ID system in the following areas:

XI.A.1. This directive;

XI.A.2. The proper collection of mobile fingerprints for identification purposes;

XI.A.3. The appropriate use and sharing of information obtained from a mobile fingerprint ID system;

XI.A.4. How the mobile fingerprint ID system directive will be enforced, including penalties for committing violations of the Directive's provisions.

XI.B. Officers must complete mobile fingerprint ID system training every three years to remain eligible to use the system. The ISP Academy shall maintain appropriate records confirming that personnel have completed training in accordance with this section.

XI.C. The ISP shall monitor relevant legislative and regulatory activity impacting mobile fingerprint ID systems and shall update this directive and training curriculum accordingly.

XII. SECURITY

XII.A. Mobile fingerprint ID systems comply with the Criminal Justice Information Systems (CJIS) Security Policy of the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division (Version 5.6 June 2017)

XII.B. Only officers authorized by the Mobile ID Coordinator may submit fingerprints through the Mobile ID system.

XII.C. System access passwords may not be shared between officers.

XII.D. The ISP is committed to protecting privacy and maintaining the integrity and security of personal information and will implement security requirements for the mobile fingerprint ID systems.

XII.D.1. Firewalls will be in place to prevent unauthorized agencies, entities, or individuals from accessing ISP resources.

XII.D.2. The ISP will monitor and respond to security breaches or breach attempts (See 815 ILCS 530/1, et seq., "Personal Information Protection Act").

XII.D.2.a. In the event ISP personnel become aware that the security of personal information has been compromised, the ISP will notify the individual about whom personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens the physical or financial harm to the person.

XII.D.2.b. Notice will be made promptly and without unreasonable delay following discovery or notification of the unauthorized access. Notice will be consistent with legitimate law enforcement needs to investigate the release or determine the scope of the release of information and if necessary, to reasonably restore the integrity of any information system affected.

XII.D.3. The mobile fingerprint ID system shall be secured in a location restricted to designated authorized personnel or secured in their squad car.

XII.D.4. Each mobile fingerprint ID capture device is subject to ISP inventory rules and directives. An officer transferring a Mobile Fingerprint capture device to another ISP employee must notify the Mobile ID Coordinator of the property transfer.

XII.D.5. All ISP personnel with access to social security numbers in the course of performing their duties will be trained on the requirements of ISP Directive SRV-200, "Information Security and Disposal of Personal Information."

Indicates new or revised items.

-End of Directive-