Tulsa Police Department

Policy #	113F	**Effective Date**	10/24/2025
Policy Name	Mobile Identification Device	**Approved Date**	10/23/2025
Approved by	*Dennis Larsen, Chief of Police*	**Previous Date**	NEW

PURPORSE OF CHANGE:

New policy.

POLICY:

The Mobile Identification (ID) Device is used to scan fingerprints from an individual to compare against existing prints in the Oklahoma State Bureau of Investigations (OSBI) Automated Fingerprint Identification System (AFIS) and the Federal Bureau of Investigations (FBI) Repository of Individuals of Special Concern (RISC) to provide a rapid positive identification to the operator or officer in the field. The possible identifications will be limited to the individuals maintained in the searched databases and do not preclude a record from existing in other biometric or name-based repositories.

For the purposes of Mobile ID, OSBI will provide a hit (red), no-hit (green) response to a Mobile ID inquiry within 30 seconds with an accepted fingerprint. RISC will provide a hit (red), no-hit (green) inconclusive (yellow) response to a Mobile ID inquiry through the OSBI AFIS system within 60 seconds.

SUMMARY: Utilizing a Mobile ID Device in the field.

APPLIES TO: All sworn personnel.

DEFINITIONS:

AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (AFIS) – the computerized Biometric matching system operated by the OSBI.

MOBILE IDENTIFICATION DEVICE or MOBILE ID DEVICE – a handheld scanning device that communicates with the OSBI AFIS and FBI RISC.

NEXT GENERATION IDENTIFICATION (NGI) – the national fingerprint system that provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses maintained by the FBI.

REPOSITORY OF INDIVIDUALS OF SPECIAL CONCERN (RISC) – a limited population of the FBI NGI, which includes but is not limited to wanted persons, sex offender registry subjects, and known or suspected terrorist.

PROCEDURES:

A. CONSENT

1. Prior to an arrest or when no court order or search warrant requires compliance, the Mobile ID Device may be used in situations where the individual to be fingerprinted gives a knowing, willing, and voluntary consent to the use of the Mobile ID Device if the person is able to give consent. .

a. The individual may limit or withdraw consent at any time;
b. If consent is withdrawn at any point before completion of scanning the individual's finger, use of the Mobile ID Device is not authorized, its use must stop immediately.

B. WITHOUT CONSENT

1. The Mobile ID Device may be used without the consent of the individual:

   a. Upon arrest of the individual;

   b. If authorized in the execution of a valid court order or search warrant;

   c. If specifically required by statute; or

   d. If the individual is unable to provide reliable identification due to physical incapacitation or defect, mental incapacitation or defect, or death (only after Medical Examiner approval) and the immediate identification of the subject is necessary for the performance of a law enforcement function.

C. AUTHORIZED USE

1. An operator of the device must be able to articulate and justify, based on the Mobile ID Device Policy, training, experience and assessment of the circumstances, the authorized and appropriate use of the Mobile ID Device.

2. Prior to an arrest or during a lawful detention, the Mobile ID Device may be used with the consent of the individual:

   a. If the officer has reasonable suspicion the individual to be printed has committed an offense;

   b. If the officer has reasonable suspicion the individual to be printed is about to commit a criminal offense and there is a justifiable and reasonable belief the fingerprint scan will establish or nullify the individual's connection to the criminal offense;

   c. If the officer has reasonable suspicion the individual to be printed is subject to an arrest warrant and there is a justifiable and reasonable belief the fingerprint scan will establish or nullify the individual's identity in the execution of the warrant;

   d. If the officer is going to cite the individual for a Traffic Code violation or other misdemeanor, or the officer lawfully detained the person, and has reasonable suspicion the individual intentionally gave a false or fictitious name, residence address, or date of birth to the officer; or

   e. If the officer has good cause to believe the individual is a witness to a criminal offense and the officer has reasonable suspicion the individual intentionally gave a false or fictitious name, residence address, or date of birth to the officer.

   f. If the person is unable to give consent under circumstances established in Section B(1)(d) of this policy.

3. Subsequent to an arrest, the Mobile ID Device may be used without the consent of the individual to verify their identity. This is done to assist the officer in determining the appropriate handling, transporting, and routing of the individual.

4. The Mobile ID Device may be used without the consent of the individual if their fingerprints are required in the execution of a valid search warrant or court order or when specifically required by statute.

a. Reasonable force may be used to gain the individual's compliance post arrest or to execute a court order or search warrant. An officer shall use the least amount of force needed to complete the scan.

b. An individual's failure to comply may constitute contempt of court and/or resisting arrest and/or failure to comply with the lawful order of a peace officer.

5. Nonstandard use of the Mobile ID Device.

a. Any nonstandard use of the Mobile ID Device shall require notification and authorization by the operator's immediate supervisor. If the immediate supervisor is unavailable, the request will be forwarded to an acting supervisor or the second level supervisor.

D. UNAUTHORIZED USE

1. The Mobile ID Device shall be used for law enforcement purposes only and may not be used for random or general investigative or intelligence gathering.

2. Officers shall adhere to all department policies when using the Mobile ID Device, including those addressing improper or racial profiling.

3. Any unauthorized use of the Mobile ID Device may result in disciplinary action.

REGULATIONS:

1. Officers may not force or coerce an individual, except as provided herein, to submit to the use of the Mobile ID Device.

2. The use of force to obtain a fingerprint is only authorized when the subject is under arrest or the officer has a warrant or court order to obtain a fingerprint. Officers should then only use the least amount of force needed to execute the warrant.

REFERENCES:

None