P.O. 249 Mobile Identification Devices			
Effective From:	06-22-2020	Effective To:	Current

P.O. 249 – *Mobile Identification Devices*

1. DEFINITIONS
   i) Louisiana Automated Fingerprint Identification System (AFIS) – a statewide, automated fingerprint identification system, which is integrated with mugshot and computerized criminal history (CCH) information managed by the Bureau of Criminal Identification and Information (BCII).
   ii) Next Generation Identification (NGI) – the repository of biometric and criminal history information that provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses maintained by the Federal Bureau of Investigation (FBI).
   iii) Repository of Individuals of Special Concern (RISC) – the FBI-CJIS (Criminal Justice Information Services) repository containing a limited population of individuals in the NGI, which includes the following: wanted persons – including the Immigration Violator File (IVF) of the National Crime Information Center (NCIC), convicted sex offenders, known or appropriately suspected terrorists, and other persons of special interest.
   iv) AFIS Mobile Identification Device (Mobile ID Device) – a handheld scanning device that communicates with AFIS and NGI.
2. PURPOSE
   i) The purpose and use of the Mobile ID Device is to scan fingerprints from a suspect to compare against existing prints in the AFIS and the FBI NGI to provide a rapid, positive on-scene identification of an individual to the officer in the field.
      a) The possible identifications will be limited to the subjects maintained in the searched databases and do not preclude a record from existing in other biometric or name-based repositories.
   ii) For the purposes of Mobile ID, AFIS and NGI will provide a hit (red), no-hit (green), or inconclusive (yellow) response to a Mobile ID inquiry. Officers should be familiar with the manufacturer's instructions of the specific device they have been assigned to understand all information provided in response to a fingerprint scan.
      a) Hit responses on a Mobile ID Device confirm that a subject has been positively identified by fingerprint comparison to existing fingerprints in AFIS and NGI. With no other information given, a hit response, alone, does not indicate the subject is a wanted person.
      b) Any indication received from the Mobile ID Device that a subject is a wanted person should be confirmed through the officer's communications center prior to taking action based solely on this response.
      c) Inconclusive responses are a result of AFIS utilizing no human intervention in the hit determination.
3. CONSENT
   i) The Mobile ID Device may be used in situations where the subject to be fingerprinted gives a knowing and willing voluntary consent to the use of the Mobile ID Device.
      a) The subject may withdraw consent at any time prior to the completion of a successful fingerprint scan.
      b) If consent is withdrawn, use of the Mobile ID Device is not authorized, its use must stop immediately, and the officer may not force or coerce the subject to submit to the use of the Mobile ID Device.
      c) Consent cannot be withdrawn after the fingerprint has been successfully scanned by the Mobile ID Device.

ii) The Mobile ID Device may be used without consent of a suspect:
    a) Upon arrest of the suspect; or
    b) If authorized in the execution of a valid search warrant.

4. AUTHORIZED USE
    i) An officer 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.
    ii) Prior to an arrest or during a lawful detention, the Mobile ID Device may be used with the consent of the suspect:
        a) If the officer has reasonable suspicion the suspect to be printed has committed, or is about to commit, a criminal offense and there is a justifiable and reasonable belief the fingerprint scan will establish or nullify the suspect's connection to the criminal offense;
        b) If the officer has reasonable suspicion the suspect 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 suspect's identity in the execution of the warrant;
        c) If the officer is going to cite the individual for a traffic violation or other misdemeanor, or the officer lawfully detained the person, and has reasonable suspicion the subject intentionally gave a false or fictitious name, residence address, or date of birth to the officer;
        d) If the officer has good cause to believe the suspect is a witness to a criminal offense and the officer has reasonable suspicion the subject intentionally gave a false or fictitious name, residence address, or date of birth to the officer.
    iii) Subsequent to an arrest, the Mobile ID Device may be used without the consent of the arrested suspect to verify the identity of the suspect.
    iv) The Mobile ID Device may be used without the consent of the suspect if a suspect's fingerprints are required in the execution of a valid search warrant or specifically required by statute.
        a) Reasonable force may be used to gain the suspect's compliance with the search warrant. An officer shall use the least amount of force needed to execute the search warrant.
    v) Nonstandard use of the Mobile ID Device
        a) Any nonstandard use of the Mobile ID Device shall require notification and authorization by the officer's immediate supervisor. If the immediate supervisor is unavailable, the request will be forwarded to an acting supervisor or the second level supervisor.
        b) Examples of nonstandard use include:
            (1) A request from an outside law enforcement agency to fingerprint a suspect in custody. The requesting agency must comply with the procedures of this policy and any other applicable department policies and procedures.
            (2) A traffic fatality investigation in which there is no other reasonable means of identifying the deceased.

5. UNAUTHORIZED USE
    i) The Mobile ID Device may not be used for random or general investigative or intelligence gathering.
    ii) Officers shall adhere to all department policies when using the Mobile ID Device, including those addressing bias-based profiling.
    iii) Any unauthorized use of the Mobile ID Device by an officer may result in disciplinary action.