Georgia Department of Public Safety
Policy Manual

SUBJECT **MOBILE BIOMETRICS**	POLICY NUMBER **6.10**
DISTRIBUTION **SWORN EMPLOYEES**	DATE PUBLISHED **8/2/2012**
	POLICY REVIEWED **12/1/2017**

6.10.1 Purpose

The Georgia Department of Public Safety will utilize mobile biometrics to assist in establishing positive identification of individuals for use in criminal apprehension, evidence and missing person location. The purpose of this policy is to outline the use and training required for this equipment.

6.10.2 Policy

It is the policy of the Georgia Department of Public Safety to provide support to its members and other law enforcement agencies with the utilization of available mobile biometric technologies capable of supporting varying missions throughout the State of Georgia.

6.10.3 Procedures

A. Organization

1. The mobile biometric system used by the state of Georgia is also known as RapidID. The RapidID was originally funded by a Department of Homeland Security grant and was procured by the Georgia Bureau of Investigation (GBI).

2. The GBI administers the RapidID system for all agencies operating in the state of Georgia.

B. System Description

1. The RapidID system is a two fingerprint identification system that searches against a centralized fingerprint database that is administered by the GBI. The database is populated with arrests made in the state of Georgia.

2. As part of this identification, automatic secondary searches of wanted files, watch lists, sex offender registries, and probation/parole lists are also included.

3. The RapidID search provides officers with an offender's arrest record at the state and national levels. Responses to searches are returned to the officer initiating the search allowing immediate access to identifying information of an individual.

C. Equipment

1. Only equipment that is certified for use by the Federal Bureau of Investigation (FBI) with mobile biometrics may be used for the RapidID system.
2. Each RapidID mobile fingerprint device must be registered with the approved GBI vendor.

D. System Administration

1. The Commander of the Criminal Interdiction Unit will act as the system administrator for the Department of Public Safety.

2. The system administrator will maintain the authority to enable or disable user accounts, monitor system use, and reset user passwords.

E. Training

1. All members assigned a mobile biometric device must successfully complete training in the use of the device as approved by the GBI.

2. All members assigned a mobile biometric device must also obtain the GCIC Terminal Operator Inquiry Level Course per the ***GCIC Operations Bulletin 2011-51 Mobile Biometric Fingerprint Identification (Rapid ID)*** prior to using the device. This certification must remain current.

F. Use

1. Mobile biometrics unit should not be used as the primary means to identify a suspect. The officer should first approach the subject and attempt to identify him/her from documents provided by the subject, i.e., driver's license or other identification.

2. Mobile biometrics may be used during four types of police citizen encounters:

   a. Consensual Encounters (communications between police and citizens involving no coercion or detention)

      1) Consent must be voluntary.

      2) Mobile biometrics may not be used at random with intent to develop probable cause of general criminal activity.

      3) Mobile biometrics should not be used as a primary means of identification when the person is in possession of valid identification documents.

   b. Investigative Detentions

      1) Reasonable suspicion that justifies a Terry stop will not be sufficient, by itself, to compel submission of fingerprints.

      2) Probable cause exists to indicate that the suspect is concealing their true identity.

   c. Arrests

   d. Deceased/unconscious or emergency identification