TYPE OF COMMUNICATION	DISSEMINATION	DESTINATION	NUMBER	PAGE OF
General Orders	Department	Directives Manual	475.00	1 3

TOPIC:	EFFECTIVE DATE	SOURCE	APPROVED BY	☒ NEW ☒ AMENDS ☒ RESCINDS 07/08/24
Rapid Identification Device	11/12/19	TPA	JDM	

475.01 PURPOSE

The purpose of this directive is to establish guidelines for utilizing Rapid Identification Device (Rapid ID) within the Department.

The issuance and use of a Rapid ID is intended to provide officers with a specialized tool to assist in the positive identification of individuals under appropriate circumstances. Officers shall be aware that there are specific requirements and guidelines for the use of Rapid ID devices.

The Rapid ID is a tool to help identify an unknown subject or to confirm a suspected false identity. The Rapid ID is only a supplemental tool used to complete an investigation.

475.02 POLICY

A. Guidelines cannot be written to incorporate every possible application for use of the Rapid ID device. Employees should exercise sound judgment keeping in mind guidelines set forth in this policy.

B. The Rapid ID device may be used in situations where the subject has voluntarily consented to be fingerprinted using the device. This includes consent given during lawful encounters.

- No legal authority is needed if consent is given.
- Requests to provide a fingerprint shall not be in the form of a “command”.

C. Tier 1 - Consent must be free and voluntary without the threat of harm or promise of benefit.

- Subject can refuse to participate.
- A subject shall not be coerced or forced to submit to a fingerprint scan.
- The consent can be withdrawn at any time by the subject. If consent is withdrawn, use of the Rapid ID device is not authorized and its use must stop immediately.

D. Tier 2 - The Rapid ID device may be used in a situation where reasonable suspicion can be articulated that the subject has committed, or is about to commit, a criminal act when there is a justifiable and reasonable belief that such fingerprinting will either establish or nullify the subject’s connection with the crime.

- The Rapid ID device should be used as quickly as possible after reasonable suspicion is established.
- A subject not under arrest shall not be forced or compelled to provide fingerprints.
- Failure to comply with the request to provide fingerprints under these circumstances is not probable cause to arrest the subject for obstruction.

E. Tier 3 - The Rapid ID device may be used in situations where the subject would otherwise be required to give traditional fingerprint samples, as in probable cause criminal arrest situations.

F. The Rapid ID device may be used in situations where the device has been specifically authorized pursuant to a valid court order.

- Where a court order requiring the use has been rendered, reasonable and safe efforts to gain compliance should be employed.

- Failure to comply may constitute contempt of court and/or obstruction of justice.

G. Use of the Rapid ID device for random or generalized investigative or intelligence gathering, with no focused case or other legitimate reason is not authorized.

H. Special care should be taken to ensure devices are not used for purposes that may lend themselves to the inference of improper "profiling."

I. Any specialized non-standard use of the Rapid ID device shall require notification and authorization of a supervisor.

J. Officers are expected to be able to articulate how they determined that use of the Rapid ID device was justified in any given situation based on policy, training, experience, and the assessment of the circumstances.

475.03 PROCEDURES

A. The Rapid ID system is a handheld, wireless supported, scanning device utilizing two-finger fingerprint identification which searches against various databases to identify a suspect or detainee. The Rapid ID system enrolls four (4) fingerprints in its database, with two (2) fingerprints being used for an identification match.

B. The Rapid ID system is accessed through the Georgia Bureau of Investigation (GBI) using a secure internet connection by authorized law enforcement personnel via a mobile fingerprint device.

C. Once a fingerprint search is submitted to the Rapid ID system, it processes the inquiry and returns either a "Hit" or "No Hit" to the mobile fingerprint device. Hits shall be handled in compliance with GCIC policy and any applicable Immigration or federal policy/rules.

D. Databases searched when fingerprints are scanned may include but are not limited to:

- GCIC database populated with persons arrested and fingerprinted in the state of Georgia;

- Repository for Individuals of Special Concern (RISC) – includes data from the FBI Wanted Persons File, National Sex Offender Registry, FBI Known or Suspected Terrorists Watch List and other persons of special interest such as persons wanted for reentering the United States after being deported for criminal reasons;

- Immigrant Violator File (IVF) – includes "wanted person categories," criminal aliens who have been deported for drug trafficking, firearm trafficking or serious violent crimes and foreign-born individuals who have violated the Immigration and Nationality Act.

E. A Rapid ID device communicates with the GBI's Rapid ID system/database.

F. If electronic prints exist in the Rapid ID database, the device checks two (2) fingerprints obtained from a suspect or detainee for positive identification and wants and warrants.

G. All department personnel using a Rapid ID device must complete the GCIC Terminal Operator Inquiry or Entry Level Course.

H. All Rapid ID device users shall be registered on the Rapid ID system with a unique username, password and fingerprint.

- Usernames shall be assigned by the department's Rapid ID system administrator. The Rapid ID system administrator will be a member of the Technology Support Unit.

- After logging in, the user is required to change their password. User passwords shall comply with all GCIC password policies.

- Password requirements:

  - Must contain at least 3 of the following: lower case letter, upper case letter, number, or special character.

  - Must be a minimum of 8 characters; cannot be a dictionary word or proper name; User ID's and passwords cannot be the same; passwords expire every 90 days; no repeating passwords for 10 passwords.

- A fingerprint will be verified each time the user logs in.

I. Issuing Rapid ID Devices

- Approval and issuance of all Rapid ID devices shall be through the Chief of Police or his/her designee.
- Only those devices which conform to the standards as set forth by the Georgia Bureau of Investigation shall be approved.
- Officers must be GCIC certified prior to being issued/using the Rapid ID system.
- A Rapid ID device shall only be used by officers who have successfully completed required training and have demonstrated proficiency in the use of the device.

J. Training shall encompass considerations and requirements for the use of the device under various circumstances including:

- Setup and maintenance procedures;
- Proper use guidelines;
- Legal issues involved with the use of the device; and
- Reporting requirements.

K. Officers operating the Rapid ID device shall ensure the security of sensitive GCIC/NCIC information is maintained from individuals not authorized to view or receive it.

L. All Rapid ID devices shall be maintained in accordance with the manufacturer's recommendations.