


FLORIDA HIGHWAY PATROL POLICY MANUAL

	SUBJECT CRIMINAL JUSTICE INFORMATION SERVICES Formerly: Florida Crime Information Center Computer Terminal	POLICY NUMBER 14.02
		ISSUE DATE 02/01/96
		REVISION DATE 03/06/15
		TOTAL PAGES 4

14.02.01 PURPOSE

To establish regulations and procedures governing the operation and use of information received from the Florida Crime Information Center (FCIC) computer terminal(s) located in all Florida Highway Patrol Regional Communication Centers (RCCs) throughout the State as well as mobile data computers and hand-held devices assigned to designated personnel that access FCIC and other Criminal Justice Information Services.

14.02.02 AUTHORITY

Except as amended herein, the provisions of the following resources are adopted by reference and incorporated within this policy.

- U.S. Department of Justice, FBI Criminal Justice Information Services (CJIS) Security Policy
- Section 282.318, Florida Statutes, Enterprise Security of Data and Information Technology
- Chapter 71A-1, Florida Administrative Code, Florida Information Technology Resource Security Policies and Standards
- Florida Department of Law Enforcement (FDLE) Criminal Justice User Agreement
- DHSMV Information Security Policy Manual

14.02.03 POLICY

It is the policy of the Florida Highway Patrol that all employees using the FCIC computer terminal and systems that access criminal justice information are trained in and abide by all policies, procedures and directives created and disseminated by FDLE, the Control Terminal Agency for the system. In addition, all employees shall follow all established policies and procedures of the Florida Highway Patrol in the operation of the terminals and systems. The RCC manager shall be responsible for proper operations of the terminal(s) assigned to that center.

14.02.04 DEFINITIONS

- A. **FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)** – Services administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS

Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Online; and the National Instant Criminal Background Check System (NICS).

- B. **CRIMINAL JUSTICE INFORMATION (CJI)** – Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:
1. Biometric Data – Used to identify individuals, to include fingerprints, palm prints, iris scans, and facial recognition data.
 2. Identity History Data – Text data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
 3. Biographic Data – Information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
 4. Property Data – Information about vehicles and property associated with crime.
 5. Case/Incident History Data – Information about the history of criminal incidents.
- C. **FLORIDA CRIME INFORMATION CENTER (FCIC)** – A statewide, computerized telecommunications system designed to provide services, information, and capabilities to the law enforcement and criminal justice community in the State of Florida. FCIC gives these agencies access to information stored in various computerized files, and through FCIC, gives them access to other criminal justice information systems nationwide.
- D. **USER AGREEMENT** – A written and signed agreement between the FDLE, Control Terminal Agency, and the Division of Florida Highway Patrol (FHP), User of the System, stating that FHP will abide by all policies and procedures in the use of the terminal and the information obtained from the system.

14.02.05 OBJECTIVES

- A. To formulate and disseminate procedures relating to the effective and efficient use of the FCIC computer terminal and CJI systems. This will enhance officer safety by providing needed information to assist members in the performance of their duties.

- B. To ensure compliance with all policies and procedures specified by the FDLE and FCIC Operations Manual, the NCIC Code Manual and the FBI CJIS Security Policy.

14.02.06 RESPONSIBILITIES

- A. The Director designated CJIS Coordination Officer shall be responsible for:
 - 1. Ensuring all new employees or contractors receive required CJIS Security Awareness training.
 - 2. Developing and implementing required training.
 - 3. Maintaining documentation of all CJIS Security Awareness training (initial and biennial).
- B. FHP sworn members and communications center personnel may be authorized access to Criminal Justice Information Systems once required training is completed. Basic Recruit and Prior-Certified Troopers receive the required certification training prior to graduation from the FHP Academy, and therefore, should not need the temporary access status.
- C. According to the CJIS Certification manual, the user must take the CJIS Certification class within six months of employment or assignment that requires access to FCIC/NCIC. During the initial six-month period, the user may access the system utilizing a temporary access status and must be under the supervision of another certified user. Therefore, communications personnel may be granted a six-month temporary access. Contractors and their employees may be authorized access to CJIS, on an as needed basis.
- D. Individuals with CJIS access are required to receive CJIS Security Awareness training within six months of their appointment or assignment and shall renew their CJIS Security Awareness training every two years.

14.02.07 PROCEDURES

- A. All messages sent or received on the computer terminal will be regarded as official business of the Division and will not be divulged to persons outside the Division unless disseminated in accordance with federal and state law, FCIC Policy, NCIC Policy, and policies outlined in the FHP Communications Policy and Procedures Manual. Recipients of criminal justice information must be validated as an authorized recipient before such information is disseminated.
- B. All messages and message formats sent over the computer terminal shall be in compliance with the policies and procedures set forth in the FCIC Manual. Failure to comply may result in disciplinary action, up to and including dismissal. In some instances, criminal charges may be brought against the employee.

- C. All information obtained from and through the FCIC system and criminal justice systems is restricted to law enforcement and for criminal justice purposes only.
- D. All employees who operate the FCIC terminal or a system that accesses FCIC/NCIC must be certified by the FDLE.
- E. Additional CJIS Security Awareness training shall be given to employees, consultants, and vendors who have access to CJIS systems.
- F. CJIS Security Awareness training is provided by FDLE via CJIS On-Line. CJIS FCIC/NCIC Full Access Certification training shall be provided by a trainer, who is part of FDLE's Information Delivery Team (IDT). The Certification training is required for those individuals who run inquiries/transactions in FCIC/NCIC systems to include eAgent, Computer Aided Dispatch (CAD), and Mobile Data Computer software interfaced with FCIC/NCIC.