ST. PETERSBURG POLICE DEPARTMENT	DATE OF ISSUE	EFFECTIVE DATE	NUMBER
GENERAL ORDER	August 2017	Immediately	**III-08**
	Distribution: All Employees		

Subject: **NATIONAL AND STATE CRIMINAL JUSTICE INFORMATION SYSTEMS**

Index as:
911 Public Safety Telecommunicator
CCH
CCIS
CJNET
Comprehensive Case Information System (CCIS)
Computerized Criminal History
Criminal Justice Network (CJNET)
DAVID
Death Master File (DMF)
DMF
Driver and Vehicle Information Database
Emergency Contact Information (ECI)
FAC
FCIC
FCIC Agency Coordinator (FAC)
Florida Crime Information Center (FCIC)
MCT/MDT
Mobile Computer Terminal (MCT)
National Crime Information Center (NCIC)
NCIC
Telecommunication Systems
Telecommunicator
Teletype Messages
Test Query Records

Accreditation Standards: 81.2.8
Cross Reference: G.O. II-17, Computers, Software and Acceptable Use of Departmental Information Systems
CJIS Memorandum: 2013-3 (January 2013)
§119.0712(2)(c), §322.20, §815.06 and §817.568, F.S.S.
15 CFR §1110.200
Replaces: G.O. III-08, National and State Criminal Justice Information Systems (April 21, 2022)

This Directive establishes how to obtain authorization for, and access to, national and state criminal justice information systems. It also explains general procedures for transmitting and receiving messages via state and national criminal justice information systems and requires the internal distribution of messages received via these systems. This Directive consists of the following sections:

I. POLICY

A. No person will have access to or query any service of CCIS or CJNET without the written authorization of their respective Bureau Assistant Chief or designee. Access to FCIC/NCIC requires FDLE certification, approval of the FCIC Agency Coordinator (FAC), and successful completion of the applicable training.

B. All employees and applicants for employment are notified of their rights prior to being fingerprinted and/or prior to a resubmission to establish a National Rap Back subscription. This notification includes the retention of fingerprints, privacy policy and the right to challenge an incorrect criminal history record (See G.O. III-08, National and State Criminal Justice Infomation Systems_Attachment D).

C. Department Coordinators for Electronic Access

1. A Terminal Agency Coordinator (TAC) will be appointed by the Manager, Emergency Communications Division to serve as the point of contact and as a representative for the Department in matters relating to FCIC/NCIC with the Florida Department of Law Enforcement (FDLE).

2. Each Bureau Assistant Chief will appoint two Point-of-Contact (POC) persons from their respective bureau (a primary and an alternate) to process requests for access to secure applications on CJNET. On behalf of their respective bureau, POCs will also act as the Department's representatives to FDLE on matters relating to CJNET.

3. A CCIS Administrator will be appointed by the Department to process requests for access and to resolve questions related to the use of the CCIS.

4. CJNET, CCIS and FCIC/NCIC will be used for law enforcement purposes only and in strict compliance with the rules and procedures of each respective data provider.

5. No person will query their own information through FCIC/NCIC for test purposes. FCIC/NCIC test records are available for training purposes and are the only records which should be queried for training/testing purposes. (See G.O. III-08, National and State Criminal Justice Information Systems_Attachment A).

6. Non-sworn employees providing real-time information from federal, state, and local crime databases to public safety personnel responding to the scene of an emergency must be certified by the Department of Health as a Public Safety Telecommunicator (PST). All requests of this nature must be fulfilled via the PST-certified members of the Emergency Communications Center.

III. DEFINITIONS

A. 911 Public Safety Telecommunicator – A public safety dispatcher or 911 operator whose duties and responsibilities include the answering, receiving, transferring and dispatching functions related to 911 calls; dispatching law enforcement officers, fire rescue services, emergency medical services, and other public safety services to the scene of an emergency; providing real-time information from federal, state, and local crime databases; or supervising or serving as the command officer to a person or persons having such duties and responsibilities. However, the term does not include administrative support personnel including, but not limited to, those whose primary duties and responsibilities are in accounting, purchasing, legal and personnel.

B. Comprehensive Case Information System (CCIS) – A statewide court case information system that allows data sharing with a government agency. It allows the ability to search by a name or case number and provides access to progress dockets and document images.

C. Criminal Justice Network (CJNET) System – A statewide telecommunications intranet separate from, but accessed through, the Internet, which is managed by the Florida Department of Law Enforcement (FDLE). CJNET provides access to various criminal justice applications and interagency electronic mail. Select applications within CJNET are secure and may require authorization through a digital certificate, user/login ID, password, etc.

D. Emergency Contact Information (ECI) – Information maintained by the DHSMV for emergency contact purposes only and is not authorized for any other use.

E. Florida Crime Information Center (FCIC) System – An intrastate telecommunication network that provides agency-to-agency communication and access to computerized information about criminals and criminal activity at the state level.

F. National Crime Information Center (NCIC) System – An interstate telecommunication network that provides agency-to-agency communication and access to computerized information about criminals and criminal activity at the national level.

G. National Rap Back Service – The Federal Bureau of Investigations Next Generation Identification NonCriminal Justice Rap Back Service provides agencies with national notifications when the following triggering events occur criminal arrests, new warrant entry and deletion which includes the individuals FBI number, sexual offender registry additions and deletions, death notice with fingerprints.

III. CCIS, CJNET AND FCIC/NCIC AUTHORIZATION PROCEDURES

A. CCIS Personnel requiring access to CCIS must complete the CCIS *Security User Agreement/Application* form. Personnel will send this form to their respective Bureau Assistant Chief or designee via their Chain-of-Command. Once approved, a copy of the form will be forwarded to the CCIS Coordinator. The Coordinator will contact the requestor and arrange appropriate access.

B. All sworn personnel, investigative assistants, crime analysts and others who substantiate a need for information provided by CJNET, FCIC and NCIC electronic data bases will be permitted to have access.

1. CJNET Application Procedures
   a. Digital Certificate Authorization – For CJNET applications requiring a digital certificate for access, users will electronically apply for authorization.
      1) Patrol Officers will contact the Information and Technology Services (ITS) Division. Others seeking access will contact their respective Division's POC.
      2) Login ID/Password Authorization – For CJNET applications requiring a user/login ID or password for access, users will contact their respective bureau POC or the ITS Division for authorization.

2. Personnel requiring access to FCIC/NCIC must successfully complete the basic FCIC/NCIC class.
   a. Class attendance is arranged through the TAC.
   b. Recertification is required at certain intervals.

IV. FCIC/NCIC INCOMING MESSAGES

A. When a message is received via FCIC/NCIC, the on-duty Echo Channel Telecommunications Operator will route a copy of the message to the appropriate unit(s) in the Department.

B. Urgent messages requiring an immediate reply will be delivered immediately to the proper unit(s) by the receiving Telecommunications Operator.

C. All crime-related "Be on the Lookout" (BOLO) messages will be sent to the Criminal Intelligence and Threat Assessment Unit in addition to other units which may have a direct interest in the information provided.

V. FCIC/NCIC OUTGOING MESSAGES

A. All messages for FCIC/NCIC originating from the Department will be provided to the Echo Channel Operator for transmittal.

1. Simple messages; *i.e.*, "message acknowledgments," may be accepted verbally.

2. Lengthy or involved messages, notifications, etc., will be given to the Echo Channel Operator in writing.

3. If quality photos of runaways, missing persons or stolen property (including vehicles and boats) are available, they will be electronically attached to the appropriate outgoing message.

4. The Echo Channel Operator will ensure that replies to messages received via FCIC/NCIC are either promptly answered or brought to the attention of their immediate supervisor or relieving operator.

VI. COMPUTERIZED CRIMINAL HISTORY (CCH) IN-FORMATION

A. Computerized Criminal History (CCH) information via FCIC/NCIC will be requested for law enforcement purposes only.

B. There are two ways to obtain CCH information:

1. Through Echo Channel or from the Records and Identification FCIC/NCIC Operator.
   a. A request may be made verbally.
   b. Replies will be given only to the person making the request, unless otherwise approved by a supervisor.
   c. CCH data printed by the operator, for the requestor's use, will be stamped with the **Criminal History Warning Stamp** (Figure 1) and the requestor will acknowledge receipt by signing the dissemination log.

WARNING
FLORIDA LAW PROHIBITS THE DISSEMINATION OF THIS CRIMINAL HISTORY INFORMATION TO ANYONE OTHER THAN ST. PETERSBURG POLICE DEPARTMENT PERSONNEL. IT IS TO BE USED FOR THE SOLE PURPOSE OF CRIMINAL INVESTIGATION. THIS REPORT MUST BE DESTROYED UPON COMPLETION OF YOUR INVESTIGATION.
YOU ARE ACCOUTNABLE FOR THIS REPORT.

Figure 1

   d. After use, the CCH data will either be returned to the system operator or destroyed by the requester.

2. CCH data may be directly obtained from FCIC/NCIC by authorized users.
   a. Users may make a direct enquiry to the FCIC/NCIC CCH database
   b. Using the appropriate purpose code.
      1) The most commonly used purpose codes are listed below.
         a) Purpose Code C- Criminal Justice. Purpose code C is used for official duties in connection with the administration of criminal justice.
         b) Purpose Code F- Weapons-Related Background Checks. Purpose code F is used by criminal justice agencies for issuing firearms-related permits and explosive permits pursuant to state law, regulation or local ordinance, returning firearms to their lawful owners, and enforcing federal and state laws prohibiting certain persons with criminal records from possessing firearms in circumstances in which firearms have been pawned.
         c) Purpose Code J- Criminal Justice Employment. Purpose Code J is used when the III/CCH transaction involves employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency is required to have management control.
      2) Authorized users utilizing purpose codes other than C, F and J must refer to the FCIC Operating Manual and/or the FCIC Agency Coordinator (FAC) to ensure proper usage of purpose codes.
   c. CCH data obtained with a mobile computer will not be printed.
   b. CCH data obtained with a desktop computer may be printed by the user.
      1) Upon receipt, it must be stamped with the **Criminal History Warning Stamp** (Figure 1); and
      2) If the CCH data is transferred to another authorized person, the transfer must be recorded and signed for on the CHH Dissemination Log.
      3) During the audit process, the FDLE will require randomly selected individual employees, both sworn and civilian, to justify the purpose for making specific requests for Criminal History Information.

C. Emergency requests may be made directly to the Echo Channel Operator for CCH data deemed necessary during a life-threatening situation, a SWAT Team incident, or when an arrest is imminent based on the criminal history information of the subject.

D. Criminal history information via FCIC/NCIC will only be transmitted over Echo Channel when that information affects an officer's safety.

VII. DRIVER AND VEHICLE INFORMATION DATABASE (DAVID)

A. Confidentiality of DAVID Information

1. The use of DAVID (Driver and Vehicle Information Database) is for official law enforcement purposes only. Therefore, employees with DAVID access must use the system for authorized purposes only. Unauthorized access, use, or disclosure of data from DAVID is a serious matter and may result in civil lawsuits and a possible violation of criminal law.

2. Unauthorized use includes, but is not limited to, queries not related to a legitimate law enforcement purpose, personal use, improper dissemination to non-law enforcement personnel, and sharing, copying or distributing DAVID information to unauthorized users. Copying or distribution of DAVID information to branches of government for the purpose of employment or risk management is not authorized use per §322.20, F.S.S.

3. Any person using DAVID will sign (electronically or in hard copy) the DAVID Confidential Acknowledgement and the Criminal Sanctions and Civil Liability Acknowledgement forms in accordance with the Memorandum of Understanding (MOU) between the St. Petersburg Police Department and the Department of Highway Safety and Motor Vehicles (DHSMV) (See G.O. II-08, National and State Criminal Justice Infomation Systems_Attachment D)

B. Emergency Contact Information (ECI)

1. The Florida Department of Highway Safety and Motor Vehicles (DHSMV) has urged Floridians to take advantage of the Agency's online system that allows them to voluntarily provide the name, address and phone number of a contact person for use by law enforcement in the event of an emergency.

2. Emergency contact information contained in a motor vehicle record is confidential and exempt from §119.07(1), F.S.S. and §24(a), Art. I, State Constitution.

3. ECI will only be used by law enforcement for emergency contact purposes.

4. All ECI requests will be routed through ECHO Channel, Emergency Communications Center.

5. ECI is not authorized for any other use, including investigative, operational, or administration of criminal justice purposes, unless used with the express consent of the person to whom it pertains.

6. Any unauthorized use of ECI will be considered a misuse of DHSMV information regardless of whether the ECI was obtained from DAVID or FCIC and may be considered a criminal violation.

C. Death Master File (DMF)

1. The use of the Death Master File (DMF) is for official law enforcement purposes only. The Social Security Administration administers the DMF but does not guarantee the accuracy of the database. Action should not be taken against any individual without further investigation to verify the death information listed.

2. Employees with access to the DMF will not:
   a. Disclose DMF information to any person who does not meet the requirements for access;
   b. Disclose DMF information to any person who uses the information for any purpose other than a legitimate business purpose;
   c. Disclose DMF information to any person who further discloses the information to any person other than a person who does not meet the requirement for access; or
   d. Use DMF information for any purpose other than a legitimate business purpose pursuant to a law.

3. Disclosure of the deceased date of an individual is punishable under 15 CFR §1110.200.

_____
Anthony Holloway
Chief of Police