



<b>Somerville Police Department</b> 		<b>TYPE:</b> <b>GENERAL ORDER</b>		<b>POLICY NUMBER:</b> <b>403</b>		<b>VERSION:</b> <b>2.00</b>	
		<b>Subject:</b> <b>Criminal Justice Information System</b>					
		<b>Issuing Authority:</b> <b>Charles Femino</b> <b>Chief of Police</b>		<b>Signature:</b> 		<b>Effective Date:</b> December 22, 2021	
		<b>Number of Pages:</b> Page 1 of 5					
<b>Accreditation Standards (6<sup>th</sup> Edition) 82.1.7</b>				<input type="checkbox"/> New <input checked="" type="checkbox"/> Revised <input type="checkbox"/> Amended			
<b>Revision &amp; Reissued Dates:</b>	2/09/2015						

## Purpose

To establish guidelines for the proper operation of fixed, remote, and portable criminal justice information system (CJIS) workstations, and to ensure the lawful handling of Criminal Offender Record Information (CORI) information generated from or maintained within the CJIS network.

## Policy

The Department of Criminal Justice Information Services (DCJIS) has strict guidelines about what information can be accessed and disseminated, and by whom. Employees of the Somerville Police Department with access to CJIS must scrupulously follow these guidelines. An employee who furnishes CORI data to any person or agency not authorized to receive it is violating the law and is subject to both criminal and/or civil penalties. In addition, CJIS access is a privilege granted to the Somerville Police Department that can be revoked.

### A. System Use

1. The use of a CJIS web portal is for criminal justice purposes only. These include the commission of official criminal justice duties like: investigations, bookings, warrant entry, qualifying an individual for employment within a criminal justice agency, and qualifying an individual to determine his/her eligibility to possess a firearms license. Use for non-criminal purposes including: transactions conducted for public and private educational establishments, municipal agencies, town government officials, is strictly prohibited and is punishable by a fine, suspension of services and/or incarceration.
2. Each user shall immediately report any damage to a CJIS workstation to a supervisor. It is the department's responsibility to report an inoperable CJIS workstation to the Office of Technology and Information Services as soon as possible. Workstation users may be held responsible for damage done to a CJIS workstation.

3. No CJIS equipment including CJIS workstations, mobile data workstations, tablets, or personal digital assistants shall be modified or altered in any way from its set-up configuration, unless it is done by the DCJIS or the device's contract vendor, and then only with notification to, and concurrence of, the DCJIS.
4. The department must ensure that all CJIS information is protected pursuant to FBI CJIS Security Policy. [82.1.7]

#### **B. System Access [82.1.7]**

1. All users of the CJIS web portal shall be trained, tested, and certified under procedures set forth by the DCJIS before using a web portal and shall be re-certified biannually thereafter.
2. Each CJIS user shall use his/her assigned password when accessing the CJIS network and shall not give this password to anyone under any circumstances. No one shall use the network under another individual's password.
3. All users, when necessary, shall log-on to the network at the beginning of the shift and shall log-off at the end of the shift to ensure that transactions are logged under the appropriate user name. This will prevent one operator from being held responsible for another operator's CJIS transactions. Appropriate care will be taken to not allow any unauthorized access to CJIS.
4. The department is obligated to monitor CJIS messages twenty-four (24) hours a day, seven (7) days a week, fifty-two (52) weeks a year, to confirm hit confirmations.

#### **Definitions**

CJIS – The Criminal Justice Information System is the database containing all information available to law enforcement.

CJIS Web portal: Any electronic device used to access CJIS sensitive data.

CORI – Criminal Offender Record Information is the database that contains a person's criminal history data.

DCJIS – The Department of Criminal Justice Information Services is the state's agency in charge of all data in the state's Criminal Justice Information System.

NCIC – The National Crime Information Center is the United States' central database for tracking crime-related information.

NICS – The National Instant Crime Background Check System is a system developed with the ATF that checks available records on individuals who may be disqualified from receiving firearms.

User – A user is a Somerville Police Department employee who is authorized to access CORI information.

## **Procedures**

### **A. CJIS Web Portal And Information Must Be Handled With Guidelines Set By:**

1. The Massachusetts General Laws
2. The Code of Massachusetts Regulations (CMR)
3. 28 code of Federal Regulations 20
4. The Massachusetts Department of Criminal Justice Information Services through manuals, training, CJIS Administrative Messages, information contained on the CJIS Extranet, and information disseminated at the Regional Working Groups meetings.

### **B. CORI**

1. The Massachusetts Public Records Law (G.L. c. 4, § 7) gives the public the right of access to most records maintained by a government agency. However, CORI information, including that which is obtained from the CJIS network is exempt from public access under the CORI Law (G.L. c. 6, §§ 167-178).
2. CORI is data compiled by a criminal justice agency concerning an identifiable individual which relates to the nature of an arrest, criminal charge, judicial proceeding, incarceration, rehabilitation or release, and may include a juvenile tried as an adult.
3. Under 803 CMR, only those officials and employees of criminal justice agencies, as determined by the administrative heads of such agencies, shall have access to CORI. Criminal justice employees are eligible to receive CORI as needed during the course of their official duties.
4. Reasons for conducting a board of probation (BOP) check may include, but is not limited to:
  - a. Investigation
  - b. Arrest
  - c. Application for criminal justice employment.

- d. Local licensing purposes e.g., door-to-door sales people.
  - e. Firearms licensing purposes.
5. An officer may share CORI with other officers or criminal justice agencies when an investigation is being conducted, however if a copy is disseminated, the dissemination must be logged in the agency's secondary dissemination log with the date, time, individual checked, purpose, officer's name, and the agency and agent to whom the information was given. The dissemination log is located in the Records Office. [82.1.7]
  6. A local municipal agency seeking CORI must apply to the DCJIS for CORI certification. If certified by the DCJIS, that agency shall submit all requests for CORI to the DCJIS.
  7. Anyone requesting a copy of his or her own CORI shall be given a form to request such information from the DCJIS, or be directed to the DCJIS Web site, [www.mass.gov/cjis](http://www.mass.gov/cjis), to print the form.
  8. Many non-criminal justice agencies have been authorized by the DCJIS to receive CORI information under G.L. c. 172(a). Such authorization was given to these agencies in writing, and a copy of this letter should be provided by these requesting agencies to the agency or police department that will be providing the requested CORI information.
  9. All other requests for CORI shall be referred to the Chief's office.
  10. To lawfully obtain CORI and to then furnish the information to any person or agency not authorized to receive is unlawful and may result in criminal and/or civil penalties (G.L. c. 6, § 177 and § 178).
  11. All complaints of CORI being improperly accessed or disseminated shall be handled as a citizen complaint and the Chief shall be advised of the matter. The complainant shall also be advised that they may file a complaint with the DCJIS by calling (617) 660-4760.

### **C. Interstate Identification Index**

1. Interstate Identification Index (III) checks may only be made for three (3) purposes:
  - a. The administration of criminal justice.
  - b. Background check of a person applying for criminal justice employment.
  - c. Background check of a person applying for an FID Card or an LTC.
2. Each agency must be able to identify a requestor of internal III inquiries.

3. Whenever III information is disseminated externally to another criminal justice agency, it must be logged in the agency's III Records Check Log with the same information provided in the Agency's Secondary Dissemination Log. Both log books are located in the Station Officers room. [82.1.7]

#### **D. NCIC Files Policy Compliance Summary**

1. Each agency must ensure that caution indicators are set properly for wanted person file entries and explained in detail under the Misc. field.
2. When entering Wanted Persons and/or Missing Persons, Vehicle, and any other records into the CJIS/NCIC system, one must make certain that all records are entered in a timely manner being sure to include all available information to create a complete record.
3. Invalid records should be removed promptly from the CJIS network to guarantee integrity of the data.
4. Every entry made into the CJIS/NCIC system should be subject to a second-party check to ensure accuracy of the record.

#### **E. National Instant Criminal Background Checks System (NICS)**

1. NICS can only be used for Firearms Licensing purposes, no other transactions are authorized. Per the FBI, 'NICS can't be used for employment screening of any type, nor can it be used for firearm releases or to check on individuals used as references for firearms related permits. Finally, the NICS cannot be used for law enforcement investigations outside the scope of the Gun Control Act in conjunction with the Alcohol Tobacco Firearms and Explosives.