Waltham Police Department
CHAPTER 13A
DCJIS

General Order Number: GO-04 04/02/2026
Effective Date: 2015/2016, 04/2017, 04/2022, 03/2024, 12/2024, 04/2026
Accreditation Standard #: 74.1.3

GENERAL CONSIDERATIONS AND GUIDELINES

The Massachusetts Department of Criminal Justice Information Services (DCJIS) provides for and exercises control over the installation, operation and maintenance of the data processing and data communication systems known as the Criminal Justice Information System (CJIS), the Criminal Offender Record Information (CORI) system and the Firearm Records Bureau (FRB).

The scope of this policy applies to any electronic or physical media containing CJI while being stored, accessed, or physically moved from the Department. This policy also applies to any authorized person who accesses, stores, and/or transports electronic or physical media containing CJI. Transporting CJI outside of the Department must be monitored and controlled.

This policy applies to all employees, contractors, temporary staff, and other workers with access to CJIS and FBI systems and/or data, sensitive and classified data, and media. This policy applies to all equipment that processes, stores, and/or transmits CJI and classified and sensitive data that is owned or leased by the DCJIS.

POLICY:

It is the policy of the Waltham Police Department to:

a. Keep/maintain direct terminal access to the Criminal Justice Information System, hereinafter referred to as, CJIS. Terminals are located in police operations and in the dispatch center.

b. Use the CJIS network for criminal justice purposes only. These include the commission of official criminal justice duties, qualifying an individual for employment within a criminal justice agency, and qualifying an individual to determine his/her eligibility to possess a firearms license. It cannot be used for non-criminal purposes including transactions conducted for educational establishments, municipal agencies, town government officials, or personal inquiries.

c. Ensure each CJIS workstation and the information obtained from it are handled in conformity to the policies and guidelines set forth by:

1. Massachusetts General Laws.

2. Code of Massachusetts Regulations (CMR).

3. Title 28 of the Code of Federal Regulations part 20.

4. DCJIS manuals and training.

DEFINITIONS:

a. **DCJIS:** Manages and administers the Commonwealth's law enforcement information and criminal records systems, the Firearms Records Bureau, and the post-conviction victim notification program.

b. **CJIS:** The computer system maintained by DCJIS which contains criminal justice information including but not limited to: criminal histories, records of wanted persons and stolen property, judicial restraining orders, and missing persons.

c. **CORI:** Records in any communicable form compiled by a criminal justice agency that concerns an identifiable individual and relate to the following:

1. Nature and disposition of a criminal charge.

2. An arrest.

3. A pretrial proceeding.

4. Other judicial proceedings.

5. Sentencing.

6. Incarceration.

7. Rehabilitation.

8. Release.

CORI shall not include:

1. Evaluation information.

2. Statistical and analytical reports.

3. Files in which individuals are not identifiable.

4. Intelligence information.

5. Any offenses that are not punishable by incarceration.

d. **CRIMINAL JUSTICE AGENCY:** Any government agency which has primary responsibility to perform duties relating to crime prevention, the apprehension, prosecution, defense, adjudication, incarceration, or rehabilitation of criminal offenders.

e. **DISSEMINATION:** The release of CJI in any communicable form.

f. **EVALUATIVE INFORMATION:** Records concerning identifiable individuals charged with a crime and compiled by criminal justice agencies which appraise mental conditions, physical conditions, rehabilitative progress, and the like which are primarily used in connection with bail, pretrial, or post-trial release proceedings. Such information is not included in CORI, and its dissemination is restricted by 803 CMR and M.G.L. ch.6, §.172 and §.178.

g. **INTELLIGENCE INFORMATION:** Records compiled by a criminal justice agency for the purposes of criminal investigations, including reports of informants, investigators, or other persons or any type of surveillance associated with an identifiable individual. Such information is not included in the compilation of CORI.

h. **ELECTRONIC MEDIA:** Includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media (e.g., thumb drive).

i. **PHYSICAL MEDIA:** Includes printed documents and imagery that contains CJI.

PROCEDURES:

a. CJIS SYSTEM ACCESS:

1. All operators of CJIS workstations shall be trained, tested, and certified under procedures set forth by the DCJIS before using a workstation and shall be re-certified each year thereafter.

2. Each CJIS workstation operator shall use one's 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 operators shall log on to the network at the beginning of their workday and shall log off at the end of their workday to ensure that transactions are logged under the appropriate username. 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. Agencies entering records into NCIC must monitor their CJIS workstations and printer(s) twenty-four (24) hours a day, seven (7) days a week, fifty-two (52) weeks a year, to perform hit confirmations.

5. Authorized personnel shall protect and control electronic and physical access to CJI while at rest and in transit.

6. The Department has implemented appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use must be reported to the on-duty supervisor.

7. All personnel must follow the established procedures for securely handling, transporting, and storing media.

8. When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, printouts, and other similar items used to process, store, and/or transmit CJI and classified and sensitive data shall be properly disposed of in accordance with the measures described herein

b. <u>FINGERPRINT REQUIREMENTS</u>:

1. based criminal record checks on all personnel prior to hire and at least once every five years thereafter. In addition, agencies must conduct fingerprint-based criminal record checks on all other individuals who have unescorted access to secure (non-public) areas of the agency prior to allowing access. These individuals include city/town IT personnel, contractors, vendors, custodians, and volunteers.

2. These background check requests are submitted either as criminal justice employment checks (for all employees of the department) or as criminal justice checks (all non-employees) and can be done on your live-scan fingerprinting device. There is no fee for these checks.

3. Important: regarding fingerprint-based background checks conducted on non-department personnel, no information received in response to a fingerprint-based check may be disseminated to the individual's actual

employer.

4. If a felony conviction of any kind exists, an employee is not to be allowed access to CJIS or to any information derived from the CJIS, and the Department is required to notify the DCJIS, in writing, as soon as practical. In the case of a non-employee, the agency must deny unescorted access to the individual.

5. If a misdemeanor conviction exists, the Department must notify the DCJIS and must request a waiver before the employee is allowed to access the CJIS or CJI, or before the non-employee is provided unescorted access to secure areas.

6. A part of their respective auditing programs, both the DCJIS and the FBI will check to ensure that the appropriate fingerprint-based background checks have been completed by the agency being audited. An agency which has not conducted these fingerprint-based checks as required will be found out-of-compliance in this area.

c. <u>CORI</u>:

1. <u>CORI INCLUSIONS AND EXCLUSIONS</u>:

a. CORI are records in any communicable form compiled by a criminal justice agency that concerns an identifiable individual and relates to the nature and disposition of a criminal charge, an arrest or other judicial proceeding including sentencing, incarceration, rehabilitation or release.

b. DAILY LOGS: Department daily logs (i.e., press logs) are not classified as CORI.

c. DECEASED PERSONS: An individual's privacy rights pursuant to the CORI statute end when the person dies.

d. STATISTICAL RECORDS AND REPORTS: CORI shall not include statistical data in which individuals are not identified and from which identities are not ascertainable.

e. JUVENILE DATA: No information concerning a person under 18 years of age is CORI unless that person is adjudicated a youthful offender under M.G.L. ch.119, §.58.

f. **EVALUATIVE INFORMATION:** CORI excludes evaluative information. The access to and utilization of evaluative information is governed by 803 CMR 204.

g. **INTELLIGENCE INFORMATION:** CORI excludes intelligence information.

h. **MINOR OFFENSES:** CORI excludes minor offenses (offenses not punishable by incarceration).

i. **PHOTOGRAPHS AND FINGERPRINTS:** CORI includes fingerprints, photographs, and other identification data which is recorded as the result of criminal proceedings; however, CORI shall not include the above information used for investigative purposes if the individual is not identified.

2. **GENERAL OVERVIEW:**

a. The Massachusetts Public Records Law 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.

b. 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.

c. Reasons for conducting a Board of Probation (BOP) check may include, but is not limited to:

1. An investigation.

2. An arrest.

3. An individual applying for criminal justice employment.

4. Local licensing purposes (i.e. where the police department is the licensing agency) and door-to-door salespeople where the municipality requires the police department to regulate.

5. Firearms licensing purposes.

d. Police Officers can share CORI with other police agencies or criminal justice agencies when conducting an investigation. However, there are certain guidelines and restrictions that must be followed:

1. The agency must log the dissemination in a secondary log (WPD Share/DCJIS RECORDS), including the date, time, purpose, and the agency and agent that received the information.

2. The disclosure must be in the interests of justice, and not prohibited by statute, rule, or court order.

3. The requester must enter into an approved Memorandum of Understanding (MOU) with the recipient.

4. The requestor must maintain a "need to know" list of authorized staff.

e. A local municipal agency (i.e., City Hall, Fire Department, CPW, Schools, Military recruiters) seeking CORI shall submit all requests to the DCJIS.

f. Anyone requesting a copy of their own CORI shall be directed to the DCJIS Web site. Massachusetts Criminal Offender Record Information (CORI) | Mass.gov

g. Many non-criminal justice agencies (e.g., Department of Children and Families) have been authorized by the DCJIS to receive CORI information under M.G.L. ch.172. Such authorization was given to these agencies in writing, and a copy of this letter should be provided by these requesting agencies to the police department that will be providing the requested CORI information.

h. All other requests for CORI shall be referred to the Chief's office.

i. To lawfully obtain CORI and to then furnish the information to any person or agency not authorized to receive CORI is unlawful and may also result in criminal and/or civil penalties.

j. 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.

3. ACCESS TO CORI:

All CORI obtained from the DCJIS is confidential, and access to the information must be limited to those individuals who have a "need to know". The Waltham Police Department must maintain and keep a current list of each individual authorized to have access to, or view, CORI (i.e., Master Roster). This list must be updated every six (6) months and is subject to inspection upon request by DCJIS at any time.

4. CORI TRAINING:

An informed review of a criminal record requires training. Accordingly, all personnel authorized to review or access CORI will be familiar with the educational and relevant training materials regarding CORI laws and regulations made available by DCJIS.

5. EMPLOYMENT CRIMINAL HISTORY SCREENING:

This policy is applicable to the criminal history screening of prospective and current employees, subcontractors, volunteers and interns, and professional licensing applicants. Where CORI checks may be part of a general background check for employment, volunteer work, and licensing purposes the following practices and procedures will be followed:

a. CORI checks will only be conducted as authorized by the DCJIS and M.G.L. ch.6, §.172, and only after a CORI Acknowledgement Form has been completed.

b. If a new CORI check is to be made on a subject within a year of his/her signing of the CORI Acknowledgement Form, the subject shall be given seventy-two (72) hours' notice that a new CORI check will be conducted.

c. CORI used for employment purposes shall only be accessed for applicants who are otherwise qualified for the position for which they have applied.

d. Unless otherwise provided by law, a criminal record will not automatically disqualify an applicant. Rather, determinations of suitability based on background checks will be made consistent with this policy and any applicable law or regulations.

6. VERIFYING A SUBJECT'S IDENTITY:

If a criminal record is received from the DCJIS, the information is to be closely compared with the information on the CORI Acknowledgement Form. If the information in the CORI record does not exactly match the identification information provided by the applicant, a determination is to be made by the Chief of Police, or his/her designee, based on a comparison of the records.

7. INQUIRING ABOUT CRIMINAL HISTORY:

In connection with any decision regarding employment, volunteer opportunities, or professional licensing, the subject shall be provided with a copy of their criminal history record, whether obtained from the DCJIS or from any other source, prior to questioning the subject about his or her criminal history. The source(s) of the criminal history record is also to be disclosed to the subject.

8. DETERMINING SUITABILITY:

If a determination is made, based on the information as provided in this policy, that the criminal record belongs to the subject, and the subject does not dispute the record's accuracy, then the determination of suitability for the position or license will be made.

Unless otherwise provided by law, factors considered in determining suitability may include, but not be limited to, the following:

a. Relevance of the record to the position sought.

b. The nature of the work to be performed.

c. Time since the conviction.

d. Age of candidate at the time of the offense.

e. Seriousness of the offense.

f. The number of offenses.

g. Whether applicants have pending charges.

h. Evidence of rehabilitation or lack thereof.

i. Any other relevant information, including information submitted by the candidate.

The applicant is to be notified of the decision and the basis for it in a timely manner.

9. ADVERSE DECISIONS BASED ON CORI:

If an authorized official is inclined to make an adverse decision based on the results of a criminal history background check, the applicant will be notified immediately. The subject shall be provided with a copy the criminal history. The subject will then be provided with an opportunity to dispute the accuracy of the CORI record.

10. SECONDARY DISSEMINATION LOGS:

All CORI obtained from the DCJIS is confidential and can only be disseminated as authorized by law and regulation. A central secondary dissemination log (WPD Share folder/DCJIS RECORDS) shall be used to record any dissemination of CORI outside this organization, including dissemination at the request of the subject.

d. INTERSTATE IDENTIFICATION INDEX (III):

1. 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 a firearms license.

2. NATIONAL CRIME INFORMATION CENTER (NCIC) FILES POLICY COMPLIANCE SUMMARY:

a. The Waltham Police Department must ensure that caution indicators are set properly for wanted person file entries and explained in detail under the Misc. field.

b. When entering wanted people, missing people, stolen vehicle, or any other records into the CJIS/NCIC system, operators must make certain that all records are entered in a timely and accurate manner

being sure to include all available information to create a complete record.

c. Invalid records should be removed or corrected promptly from the CJIS network to guarantee integrity of the data.

d. Any record that needs to be cleared, such as a located missing person, a cleared warrant, a located stolen vehicle, shall be cleared in a timely and accurate manner.

3. NATIONAL INSTANT CRIMINAL BACKGROUND CHECKS SYSTEMS SURVEY (NICS):

NICS can only be used for firearms licensing purposes, no other transactions are authorized. Per the FBI, NICS cannot be used for employment screening of any type and cannot be used for law enforcement investigations outside the scope of the Gun Control Act of 1968.

e. HANDLING OF CJI:

1. PROTECTION OF CJI: To protect CJI, every employee, contractor, intern, and temporary worker shall:

a. Securely store electronic and physical media containing CJI within a locked drawer or cabinet when away from the work area. Employees with offices must lock their office doors when away.

b. Restrict access to electronic and physical media to only authorized individuals who have a need to know.

c. Physically protect CJI until media end of life. End of life CJI is to be destroyed or sanitized using approved equipment, techniques, and procedures.

d. Not use personally owned devices to access, process, store, or transmit CJI unless pre-approved by the Chief of Police in writing.

e. Not utilize publicly accessible computers to access, process, store, or transmit CJI.

f. Store all hardcopy CJI printouts in a secure area accessible to only those employees whose job functions require them to handle such documents.

g. Take appropriate action when in possession of CJI while not in a secure area:

1. CJI must not leave the employees' immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.

2. Precautions must be taken to obscure CJI from public view, such as by means of a file folder for hard copy printouts. For electronic devices like laptops, use session locks and/or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of a physically secure location, the data shall be immediately protected using encryption.

3. When encryption is employed, the cryptographic module used shall be certified to meet Federal Information Processing Standards (FIPS) 140-3 standards.

Security Requirements for Cryptographic Modules

4. Lock or log off computers when not in the immediate vicinity of the work area to protect CJI.

2. **TRANSPORT OF CJI:** Only sworn employees and authorized contractors are permitted to transport CJI outside of the Department. Each employee and contractor will take every precaution to protect electronic, physical media or copies containing CJI while in transport and/or to prevent inadvertent or inappropriate disclosure and use. Sworn employees and authorized contractors shall:

a. Protect and control electronic and physical media during transport outside of controlled areas.

b. Restrict the pickup, receipt, transfer, and delivery of such media only to authorized personnel.

c. Include privacy statements in electronic and paper documents.

d. Secure hand carried, confidential electronic and paper documents by:

1. Storing the documents, or the electronic media containing the documents in a closed handbag, laptop bag, brief case, etc.

2. Viewing or accessing the CJI only in a physically secure location.

3. Packaging hard copy printouts in such a way as to not have any CJI information viewable.

4. Mailing or shipping CJI only to authorized individuals; the package shall not be labeled "CONFIDENTIAL"; packages containing CJI material are to be sent by U.S. Mail with tracking information or by another shipping method(s) that provides for complete shipment tracking.

5. Not taking CJI home or when travelling unless necessary and approved by the Division Commander.

3. INADVERTENT OR INAPPROPRIATE DISCLOSURE OF CJI:

If CJI is unintentionally or improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

a. You shall verbally notify the Patrol Supervisor immediately. Then the DCJIS representative or back up shall be notified via email.

b. The Patrol Supervisor will communicate the situation to the Patrol Commander, and the DCJIS representative or back up, who will review the incident and will implement disclosure procedures if required, by notifying the FBI CJIS Chief Information Security Officer (CISO).

4. DISPOSAL OF CJI:

a. **PHYSICAL MEDIA:** Printouts and other paper physical media shall be disposed of by shredding.

b. **ELECTRONIC MEDIA:** Hard drives, tape cartridges, CDs, printer ribbons, flash drives, printer and copier hard-drives will be properly disposed of by the City of Waltham Office of Information Technology using one or more of the following methods:

1. Overwriting (at least 3 times).

2. Degaussing.

3. Destruction (e.g., crushing, disassembling).

c. IT systems that have been used to process, store, or transmit CJI shall not be released from the Department's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

d. Any employee who has any type of electronic media to be destroyed or discarded is to notify the Commander of the Administration Division to arrange for proper disposal.

5. PENALTIES FOR IMPROPER ACCESS, DISSEMINATION AND HANDLING OF CJIS DATA:

a. An employee who improperly accesses or disseminates CJIS data will be subject to corrective disciplinary action.

b. In addition to any penalty imposed by this department, a CJIS user may be subject to federal and state civil and criminal penalties pursuant to M.G.L. ch.6, §§.167A(d), 168 and 178 and 28 CFR 20.

f. SECURITY:

Massachusetts criminal justice agencies are reminded that any security incidents involving access, or potential access, to department systems or network, or to criminal justice information of any kind, must be reported within forty-eight (48) hours to the DCJIS, regardless of whether the incident involved the CJIS network or CJIS systems. This requirement is contained within the CJIS User Agreement, which is signed by the Department Agency Head, CJIS Representatives, and CJIS Technical Contact. Specifically:

1. INCIDENT REPORTING:

If a data breach or security violation occurs within a system that contains CJI data, a notification must be immediately sent to the appropriate CJIS agency detailing the nature of the breach, the affected data, and the steps being taken to mitigate the issue. This notification is crucial to comply with the CJIS Security Policy and prevent further dissemination of sensitive criminal justice information. The following information lists what to do in the event of a breach:

a. Notify the Department CJIS representative or their back-up. Anyone who witnesses the breach must also submit a complaint form by going to: https://www.mass.gov/how-to/report-improper-access-or-use-of-a-criminal-record.

b. Notification should be made as soon as the breach is discovered without unnecessary delay to DCJIS at 617-660-4600.

A failure to report a breach can lead to legal penalties and sanctions, including fines and potential criminal charges. Agencies found in violation of CJIS security standards may lose access to critical criminal justice databases.

2. UNESCORTED ACCESS:

To verify identification, state of residency and national fingerprint-based record checks shall be conducted. This shall be done prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing).

3. PHYSICAL SECURITY:

a. **PHYSICAL PROTECTION:** Each CJIS agency must have a written physical protection policy, along with written procedures to ensure that criminal justice information (CJI) and information system hardware, software, and media are physically protected through access control measures.

b. **PHYSICALLY SECURE LOCATION:** A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

The physically secure location is subject to criminal justice agency management control, the FBI CJIS Security addendum, or a combination thereof.

c. **SECURITY PERIMETER:** The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured in a manner acceptable to the DCJIS.

d. **PHYSICAL ACCESS AUTHORIZATIONS:** The agency shall develop, and keep current, a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

e. **PHYSICAL ACCESS CONTROL:** The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

f. **ACCESS CONTROL FOR TRANSMISSION MEDIUM:** The agency shall control physical access to information system distribution and transmission lines within a physically secure location.

g. **ACCESS CONTROL FOR DISPLAY MEDIUM:** The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

h. **MONITORING PHYSICAL ACCESS:** The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

i. **VISITOR CONTROL:** The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall always escort visitors and monitor visitor activity.

j. **DELIVERY AND REMOVAL:** The agency shall authorize and control information system-related items entering and exiting the physically secure location.

k. **CONTROLLED AREA:** If an agency cannot meet all the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.

2. Lock the area, room, or storage container when unattended.

3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from accessing and/or viewing it.

4. Follow the encryption requirements found in the FBI CJIS Security Policy for electronic storage (i.e. data "at rest") of CJI.

4. USER ACCOUNT VALIDATION:

The Chief of Police or their designee is responsible for ensuring that all active user accounts which allow access to the internal DCJIS network and its resources are valid. To that end, the Commissioner of DCJIS and/or designee shall request and review a list of all active user accounts at least once every six (6) months. As part of the review, everyone associated with an active account is:

a. Currently employed by the Waltham Police Department.

b. Authorized to access the internal DCJIS network and resources.

c. Has the appropriate access level to the network, its resources, and to directories, folders, files, etc.

d. Has had a fingerprint-supported criminal background check conducted on them within the last five (5) years. Sworn officers will have this check conducted at the same time as their LTC renewal. Civilian employees are required to have this check conducted in accordance with the schedule set forth by the Waltham Police Department DCJIS Coordinator.

e. In the case of those individuals with access to CJIS resources, services and data, must pass the CJIS Security Test annually. Any user account with greater access to the network or its resources than the duties of its owner will be adjusted appropriately within 72 hours.

f. Civilians and contractors must take one of the tests listed below. If the test is not taken, they will need to be escorted throughout the

building. This includes, but is not limited to IT staff, custodians, bail clerks, and clinicians. An example of which test someone would have to take is as follows:

1. **BASIC ROLE:** Personnel with unescorted access to a physically secure location. (This level is designed for people who have access to a secure area but are not authorized to use CJI)

2. **GENERAL ROLE:** All personnel with access to CJI. (This level is designed for people wo are authorized to access an information system that provides access to CJI)

3. **PRIVILEDGED ROLE:** Personnel authorized to perform security-relevant functions. (This level is designed for all information technology personnel including system, security, network administrators, etc.)

4. **SECURITY ROLE:** Organizational personnel with security responsibilities. (This level is designed for personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJIS Security Policy)

   The tests can be found on www.CJISonline.com