



Jeffrey R. Gahler,  
Sheriff

# HARFORD COUNTY SHERIFF'S OFFICE ADMINISTRATIVE POLICY

## FBI Criminal Justice Information System Security and Training

<b>Distribution:</b>	<b>All Personnel</b>	<b>Policy Number:</b>	<b>ADM 1107</b>		
<b>Responsible Unit:</b>	<b>Security Systems Administrator</b>	<b>Rescinds:</b>	<b>NEW</b>		
<b>Original Issued Date:</b>	<b>11/06/24</b>	<b>Revision #:</b>	<b>N/A</b>	<b>Latest Revision Date:</b>	<b>11/06/24</b>
<b>Latest Required Review was Completed:</b>		<b>11/06/24</b>	<b>Next Review Due:</b>		<b>11/06/27</b>

### 1. Purpose

To establish guidelines and procedures for Federal Bureau of Investigation (FBI) Criminal Justice Information System (CJIS) Security and Training for the Harford County Sheriff's Office (HCSO) as mandated by the FBI CJIS Security Policy.

### 2. Policy

All individuals who require unescorted access to any HCSO Agency facility must have CJIS fingerprints on file, must have had a full background check and the designated level of Security Awareness Training. This requirement includes all Agency personnel, regardless of rank or position, vendors, contractors, interns, etc. that require unescorted access to Agency facilities.

### 3. Definitions

**AUTHORIZED PERSONNEL:** those persons, sanctioned by the HCSO, or by a representative designated by the Sheriff of Harford County, to perform specified duties; or those persons who have an agreement or contract with the Sheriff's Office, either on a temporary or permanent basis.

**CRIMINAL JUSTICE INFORMATION (CJI):** a 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.

**CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS):** is a computerized system maintained by the Department of Justice (DOJ) in each state and includes the National Crime Information Center (NCIC), Uniform Crime Reporting (UCR), the Integrated Automated Fingerprint Identification System (IAFIS), NCIC 2000, and the National Incident-Based Reporting System (NIBRS). The CJIS can be accessed through any of the three law enforcement communication systems: NCIC, a more localized state criminal information system (name varies by state), and the International Law Enforcement Telecommunications System (INLETS).

**CJIS SYSTEMS AGENCY (CSA):** the CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). In Maryland, the Maryland State Police (MSP) is the CSA for the State.

**CJIS SYSTEMS AGENCY INFORMATION SECURITY OFFICER (CSA ISO):** serves as the security point of contact to the FBI CJIS Division ISO. Documents technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user

community throughout the CSA's user community, to include the local level. In Maryland, the Department of Public Safety and Correctional Services (DPSCS) assigns the CSA ISO.

**CJIS SYSTEMS OFFICER (CSO):** an individual located within the CSA responsible for the administration of the CJIS network for the CSA. The CSA may delegate responsibilities to subordinate agencies.

**ESCORT:** an escort is defined as an authorized person who always accompanies a visitor while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein.

**LOCAL AGENCY SECURITY OFFICER (LASO):** designated by the Sheriff of Harford County to use the state approved hardware, software, and firmware, and who ensures no unauthorized individuals or processes have access to the same. The LASO will identify and document how the equipment is connected to the state system; ensure that personnel security screening procedures are being followed as stated in this policy; and ensure the approved and appropriate security measures are in place and working as expected.

**PERSONAL IDENTIFIABLE INFORMATION (PII):** information which can be used to distinguish or trace and individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such a date and place of birth, or mother's maiden name.

**TERMINAL AGENCY COORDINATOR (TAC):** the TAC serves as the point-of-contact at the local Agency for matters relating to CJIS Information access. The TAC administers CJIS systems programs within the local Agency and oversees the Agency's compliance with CJIS systems policies. For HCSO, the TAC Officer is the Security Systems Administrator (SSA). That position is housed within the Records Unit.

**VISITORS:** a person who visits a HCSO facility on a temporary basis who is not employed by the HCSO, or a county employee who has not been granted regular access to HCSO facilities, and who has no unescorted access to a physically secure location within the HCSO where FBI CJI and associated information systems are located.

**NOTE:** The following type of data are exempt from protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

#### **4. References**

FBI CJIS Security Policy version 5.9.4

#### **5. Procedure**

##### **A. Awareness and Training**

1. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJIS and the systems which process CJI.
2. The HCSO must provide role-based security and privacy training to personnel with the following roles and responsibilities:
  - a. All individuals with unescorted access to a physically secure location;

- b. General User: A user, but not a process, who is authorized to use an information system;
  - c. Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform; and
  - d. Organizational Personnel with Security Responsibilities: 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.
3. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and when required by system changes.

B. Responsibilities of the Agency Security Systems Administrator (SSA) include:

- 1. Receives emails from the Human Resources Director for any new hires, retirements, resignations, etc.;
- 2. Receive notifications from the IT Director, Detention Center Staff, Harford County Government Facilities, etc., for any vendors or contractors that need unescorted access. If the individual has an email account, they can be entered into the CJIS Online system as an Agency user or a vendor user. If they do not have email, the individual will use the printed training material;
  - a. The SSA will enter all new hires, vendors, contractors, etc. into the CJIS Online system, send an email to the new personnel advising them of this mandatory training and ensure they complete the training;
  - b. Any personnel who are ending their employment with HCSO will be deactivated in the CJIS Online system;
- 3. Ensuring those with unescorted access to HCSO facilities have the proper fingerprints, background check and Security Awareness Training;
- 4. Maintaining training records in CJIS Online for those users who are enrolled in that system and through an excel database for those individuals who use printed training materials; and
- 5. Periodically reviewing the training records. Three months prior to the user expiration, the SSA will send notifications out to the appropriate personnel advising them they are coming close to their expiration date, and they need to renew their certification. The SSA will provide personnel with a due date to complete the training.

C. Security Awareness Training Methods

- 1. CJIS Online website
  - a. This is used by all Agency personnel and also others with unescorted access who have an email account.
- 2. Printed training materials
  - a. This is used by individuals who do not work for HCSO and do not have an email address to use for the CJIS Online website.

- b. These users must review the training material and sign the CJIS Security Awareness Training Agreement. This agreement will be given to the SSA for documentation, tracking, and CJIS Audit purposes.

#### D. Security Awareness Training Roles


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. Examples include janitors, contractors – anyone who cannot log on to an HCSO computer.
2. **General Role:** All personnel with access to CJI. This level is designed for people who are authorized to access an information system that provides access to CJI. Examples include all HCSO employees except for LASO, IT Personnel, TAC and back up TAC's – this is anyone who can log on to an HCSO computer – including vendors and contractors with HCSO computer access.
3. **Privileged Role:** Personnel authorized to perform security-relevant functions. This level is designed for all information technology personnel including system administrators, security administrators, network administrator, 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. Examples include all HCSO IT Personnel, LASO, TAC and backup TAC's.

#### E. Physical Access Authorization

1. Only authorized personnel will have access to physically secure non-public locations.
2. The HCSO will maintain and keep current a list of authorized personnel. Those persons wishing to have physical access into the Agency's secure areas must be authorized before being granted access. The Agency will implement access controls and monitoring of physically secure areas for the protection of all transmission and display mediums of CJI. All physically secure access points will be identified.
3. Authorized personnel will take necessary steps to prevent and protect the Agency from physical, logical, and electronic breaches.
4. All personnel with CJI physical and logical access must meet the minimum personnel screening requirements prior to CJI access.
5. To verify identification, a state of residency and national fingerprint-based record checks will be conducted before they can have unescorted access to any of the computer systems with access to CJI.
6. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) will be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.
7. Prior to granting access to CJI, the HCSO, on whose behalf the contractor is retained, will verify identification via a state of residency and national fingerprint-based record check.

F. Security Awareness

1. All authorized HCSO private contractor/vendor employees will receive security awareness training before being granted unescorted access and then every year thereafter. Security awareness training will cover areas specified in the CJIS Security Policy at a minimum, including:
  - a. Awareness of who is in their secure area before accessing confidential data;
  - b. Taking appropriate action to protect all confidential data;
  - c. Protection of all terminal monitors with viewable CJI displayed and not allowing viewing by the public or escorted visitors;
  - d. Protection from viruses, worms, Trojan horses, and other malicious code;
  - e. Web usage - allowed versus prohibited; monitoring of user activity (allowed versus prohibited is at the Agency's discretion); and
  - f. Not using personally owned devices on the HCSO computers with CJI access.
2. Use of electronic media is allowed only by authorized HCSO personnel. Controls will be in place to protect electronic media and printouts containing CJI while in transport.
3. When CJI is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.
4. Hard copy printouts of CJI will be released only to authorized vetted personnel who will shred or burn hard copy printouts when no longer needed.
5. When CJI access is no longer needed, HCSO security personnel will be informed. In the event of ended employment, the individual must surrender all property and access managed by the local, state, and/or federal agencies.

Approved  
  
JEFFREY R. GAHLER  
SHERIFF  
DATE 11-6-24