

GENERAL ORDER



DISTRICT OF COLUMBIA

Subject CJIS Security		
Topic	Series	Number
SPT	302	12
Effective Date March 28, 2014		
Related to: GO-SPT-302.08 (Metropolitan Police Department (MPD) Wide Area Network) General Order 302.06 [The Washington Area Law Enforcement System (WALES)]		

I.	Background	Page	1
II.	Purpose	Page	1
III.	Definitions	Page	2
IV.	Regulations	Page	2
V.	Procedures	Page	3
V.A	Requests for CJIS Access	Page	3
V.B	Background Checks	Page	3
V.C	Access Control	Page	5
V.D	Security Awareness Training	Page	7
V.E	Physical and Digital Disposal	Page	8
VI.	Cross References	Page	9

I. BACKGROUND

The Metropolitan Police Department (MPD) has been designated by the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division, as the CJIS System Agency (CSA) for the criminal justice community of Washington D.C. As the designated CSA, MPD is responsible for establishing and administering a CJIS security program throughout their CJIS user community. MPD is responsible for setting, maintaining, and enforcing standards and policy that govern the operations of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support the telecommunications network and related CJIS Systems used to process, store or transmit criminal justice information (CJI).

II. PURPOSE

The purpose of this order is to establish the security policies and procedures governing the operation of CJIS consistent with the FBI's *Criminal Justice Information Services (CJIS) Security Policy*. This order will ensure the integrity and availability of CJIS services and continuity of information protection.

III. DEFINITIONS

When used in this directive, the following terms shall have the meanings designated:

1. Access Control – Security characteristic that controls access levels to resources within CJIS. Access control provides the planning and implementation of mechanisms to restrict reading writing, processing and transmission of CJIS information and the modification of information systems. Application, services and communication configuration allow access to CJIS information.
2. CJIS System Agency (CSA) – Agency responsible for administering and safeguarding criminal justice information and its technology services throughout the CSA's user community.
3. CJIS Systems Officer (CSO) – Individual located within the CSA responsible for the administration of the CJIS network for the CSA.
4. Contractor – Non-MPD agency (to include other District government agencies), private business, or individuals that have entered into an agreement with the CSA or an external user agency and has either physical or logical (i.e., remote) access to CJI.
5. Member – MPD sworn or civilian employee or Reserve Corps member.
6. Physically Secure Location – Facility or area, room, or group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

IV. REGULATIONS

- A. The requirements of this order apply to all members who have access to unencrypted CJI including those individuals with only physical or logical (i.e., remote) access.
- B. Members shall be subject to the requirements of this order in addition to, and not in place of, other applicable laws, MPD policies and procedures, and the Federal Bureau of Investigations' *Criminal Justice Information Services (CJIS) Security Policy*.
- C. Members of the public **must** be escorted by authorized members (i.e., members with authorized CJIS access) at all times while visiting the computer center or any area that has CJIS terminals and CJIS data. A log will be kept of all visitors.
- D. The MPD Chief Technology Officer shall appoint a CJIS Systems Officer (CSO).

- E. The CSO shall be responsible for ensuring compliance with the requirements of this order and the Federal Bureau of Investigation's *Criminal Justice Information Services (CJIS) Security Policy*.
- F. The CSO shall ensure periodic audits are conducted to ensure compliance with this order.

V. PROCEDURES

A. Requests for CJIS Access

- 1. The CSO or his/her designee shall have approval authority for all internal requests for access to CJIS. All designees to the CSO shall be from authorized Criminal Justice Agencies (CJA).
- 2. The CSO shall ensure that a user agreement is entered into for any outside agency who receives access to CJIS/WALES.

B. Background Checks

- 1. The CSO shall ensure that within thirty (30) days of a member being granted access to criminal justice information (CJI) or being assigned responsibility to configure and maintain computer systems and networks with direct access to CJI:
 - a. The member's identification and state of residency are verified.
 - b. A national finger-based record check is conducted on the member.
 - (1) If a felony conviction of any kind exists, access to CJI shall be denied. However, in extenuating circumstances, the CSO may grant access where the severity of the offense and the time that has passed would support a possible variance.
 - (2) If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
 - (3) If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access is appropriate.

- (4) If the person is employed by a Non-criminal Justice Agency (NCJA), the CSO or his/her designee, and, if applicable, the appropriate board maintaining management control, shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction.
 - (5) If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSO, only the authority to grant access to CJI.
 - (6) If the CSO or his/her designee determines that access to CJI by the person would not be in the public's best interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
2. The CSO shall ensure that a WALES/NCIC check is performed, at minimum, every five (5) years for members with access to CJI or being assigned responsibility to configure and maintain computer systems and networks with direct access to CJI.
3. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.
4. Screening for Contractors
 - a. Prior to granting a contractor access to CJI, the CSO of the Contracting Government Agency (CGA) on whose behalf the contractor is applying shall verify identification via state residency and national fingerprint-based record check.
 - b. If a record of any kind is found, the CGA will be formally notified, and system access will be delayed pending review of the criminal history record information. The CGA will in turn notify the contractor-appointed Security Officer.
 - c. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA of the CJA will review the matter. A contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified. Applicants shall also be disqualified on the basis of

confirmations that arrest warrants are outstanding for such applicants. Applicants with a record of misdemeanor offense(s) do not warrant disqualification.

- d. The CGA may request the CSO review a denial of access determination.
- e. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of access list to the CSO.

C. Access Control

1. CJIS Accounts

- a. The CSO shall ensure CJIS accounts are established, activated, modified, reviewed, disabled, and removed in accordance with this order.
- b. The CSO shall ensure CJIS account rights and privileges are granted and removed based on established criteria.
- c. The CSO shall ensure all CJIS accounts are validated at least annually and shall document the validation process.
- d. The CSO may delegate the responsibility to other agencies of the validation and documentation of accounts for their members.

2. System Use Notification

- a. The CSO shall ensure that the information system displays an approved system-use notification message before granting access, informing potential users of various usages and monitoring rules.
- b. The system-use notification message shall, at minimum, provide the following information:
 - (1) The user is accessing a restricted information system.
 - (2) System usage may be monitored, recorded, and subject to audit.
 - (3) Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
 - (4) Use of the system indicates consent to monitoring and recording.

3. The CSO shall ensure:
 - a. The perimeters of physically secure locations are prominently posted and separated from non-secure locations by physical controls.
 - b. Security perimeters are defined, controlled and secured in a manner acceptable to the CSA.
 - c. A list is developed and kept current of personnel with authorized access to physically secure locations (except for those areas within the permanent facility officially designated as publicly accessible) or shall ensure credentials are issued to authorized personnel.
 - d. Physical access points (except for those areas within the facility officially designated as publicly accessible) are controlled and individual access authorizations are verified before granting access.
 - e. Physical access to information system distribution and transmission lines is controlled within physically secure locations.
 - f. Physical access to information system devices that display CJI are controlled and information system devices are positioned in such a way as to prevent unauthorized individuals from accessing and viewing.
 - g. Physical access to the information system is monitored to detect and respond to physical security incidents.
 - h. Physical access is controlled by authenticating visitors before authorizing escorted access to physically secure locations (except for those areas designated as publicly accessible).
 - i. Visitor access records to physically secure locations (except for those areas officially designated as publicly accessible) are maintained that include:
 - (1) Name and agency of the visitor;
 - (2) Form of identification;
 - (3) Date of access;

- (4) Time of entry and departure;
 - (5) Purpose of visit; and
 - (6) Name and agency of person visited.
- j. Visitor access records are maintained for a minimum of one (1) year and designated officials within the agency review the visitor access records frequently for accuracy and completeness.
 - k. Information system-related items entering and exiting physically secure locations are authorized and controlled.
 - l. Electronic and physical media that contain CJI (e.g., hard drives and jump drives) are protected and controlled during transport outside of controlled areas and the activities associated with transport of such media are restricted to authorized personnel.

D. Security Awareness Training

- 1. The CSO shall ensure that all new members who have access to CJIS systems and information and all appropriate MPD Office of the Chief Technology Officer members receive security awareness training within six (6) months of their appointment or assignment.
- 2. The CSO shall ensure that security awareness training is provided at least once every three (3) years to all members who manage or have access to CJIS systems and information.
- 3. The CSO shall ensure CJIS security awareness training addresses, at minimum, the following topics:
 - a. Relevant terminology including, but not limited to, information system, information technology security, CSA and CSO;
 - b. *Criminal Justice Information Services (CJIS) Security Policy*;
 - c. Desktop security;
 - d. Passwords;
 - e. Storing of sensitive data;
 - f. Disposal of sensitive data; and
 - g. Vulnerabilities, threats and sanctions.

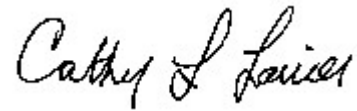
4. The CSO shall maintain an updated schedule including the last training/certification dates of all members who have received security awareness training.
5. The CSO may terminate CJIS Access for any members who fail to comply with CJIS training requirements.
6. External Agencies and Contractors
 - a. The CSO shall ensure that external user agencies and contractors:
 - (1) Administer and maintain their own security awareness training curriculum that meets the components of the FBI's *Criminal Justice Information Services (CJIS) Security Policy*.
 - (2) Provide their training curriculum to the CSO for review.
 - b. The CSO shall ensure that upon the biannual audit provided by the CSA, all external user agencies and contractors provide dates of security awareness training certifications.

E. Physical and Digital Data Disposal

1. The CSO shall ensure the tracking and disposal of physical and digital data complies with the *Criminal Justice Information Services (CJIS) Security Policy*.
2. Data disposal records shall be maintained that include:
 - a. Name of person destroying data. The person must be CJI-cleared;
 - b. Origin of the data, type, make, model. (e.g., paper, hard disk);
 - c. Date of destruction;
 - d. Destruction method; and
 - e. Disposal method.
3. Destruction records shall be maintained for a minimum of four (4) years and designated officials within the agency shall review the destruction records frequently for accuracy and completeness.

VI. CROSS REFERENCE

Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, August 9, 2013 – <http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view>.

A handwritten signature in black ink that reads "Cathy L. Lanier". The signature is written in a cursive, flowing style.

Cathy L. Lanier
Chief of Police

CLL:PAB:MOC:PHC