CJDN Network Security

Version: 04/17/2017	Document Number: MNJIS-5002	Distribution: BCA

Policy Statement / Objective:

The Bureau of Criminal Apprehension's (BCA) Minnesota Justice Information Services (MNJIS) operates the Criminal Justice Data Communications Network (CJDN) so that authorized agencies can retrieve criminal justice information (CJI) in order to perform their duties. The purpose of this policy is to help those authorized agencies comply with both the current FBI *CJIS Security Policy* (CSP) and this Bureau of Criminal Apprehension (BCA) MNJIS *CJDN Network Security Policy 5002*. The CSP provides the minimum level of information technology (IT) security requirements acceptable for the transmission, processing, and storage of the nation's Criminal Justice Information System (CJIS) data. These requirements are necessary to establish uniformity and consistency in safeguarding CJI which is accessed via networks throughout the federal, state, and local user communities.

The primary intent of this policy is to clarify certain sections of the CSP so that it is easier for agencies to be in compliance and to set statewide standards regarding the security and movement of CJI within Minnesota.

Any security controls listed in this policy that are more restrictive than the CSP will be clearly stated (they are highlighted with ***bold and italics***).

Definitions:

Many of the terms used in this policy are defined in the CSP and so are not defined in this document. Additional defined terms are found below.

Authorized agency: a government agency authorized by the BCA to have access to BCA and FBI resources and that has a valid joint powers agreement or other contract executed by it and the BCA.

BCA: The CJIS Systems Agency (CSA) and State Identification Bureau (SIB) for Minnesota.

CJI Environment: an authorized agency's isolated infrastructure where CJI passes is accessed, and/or stored. This includes, but is not limited to, network switches, routers, firewalls, workstations, servers, and virtual environments.

CJIS Systems Officer (CSO): the BCA employee responsible for the administration of the system that makes it possible to send and retrieve CJI.

Criminal Justice Data Communications Network (CJDN): For statutorily authorized users, the CJDN is a connectivity method that has been approved by the BCA.

Criminal Justice Information (CJI): Criminal Justice Information is the abstract term used to refer to all data from systems containing, integrated with, or derived from data in the FBI CJIS repositories and also includes data contained in, integrated with or derived from data maintained in BCA repositories and that are necessary for authorized agencies to perform their work.

Foreign network: any network or network connection procured only by a Local Agency that has access to the CJDN.

Local Agency: any Minnesota agency, including federal agencies that serve part or all of Minnesota, authorized to access the CJDN.

MNJIS Terminal: any device used by a Local Agency to connect to the CJDN to retrieve CJI. Examples of a MNJIS Terminal include, but are not limited to, a desktop computer, laptop, tablet, and cellular telephone.

Mobile Devices – any portable device used to access CJI via a wireless connection. Examples of mobile devices are smart phones, cellular phones transmitting CJI, laptops and tablets and other portable equipment which can easily be moved from one location to another.

Non-Physically Secure Location - a non-physically secure location is any area that does not fall under the definition of a Physically Secure Location.

Occasional Unescorted Access is the infrequent access needed for a task in a Physically Secure Location. Examples are maintaining vending machines and watering plants.

Physically Secure Location: a facility, an area, a room, or a group of rooms that have the physical and personnel security controls sufficient to protect CJI and the associated information system subject to the authorized agency's management and control. Specific information on squad cars and physical security is found on page 6.

Public Key Infrastructure (PKI) – algorithms and encryption that use key pairs to secure CJI whether in transit or at rest.

Wireless Technology is the transmission of voice and/or data communications via radio frequencies.

Policy:

This policy addresses the secure operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a data network, telecommunications network and related MNJIS systems used to process, store, share, or transmit CJI, guaranteeing the priority, integrity, and availability of service needed by state and local agencies. This policy also applies to CJI data held by authorized agencies, regardless of the means of storage.

Roles and Responsibilities:

A. CJIS System Agency Information Security Officer (CSA ISO)

1. The CSA ISO is a BCA employee who is responsible for:
    a. Ensuring agencies conform to the CSP and this policy.
    b. Ensuring management controls are in place for the CJDN including the management of State routers, firewalls, and VPN devices.
    c. Ensuring that state and local agency network topology documentation is current.
    d. Supporting security-related configuration management for the BCA and Local Agencies.
    e. Providing guidance in implementing security measures at the local level.
    f. Disseminating security-related training materials to local agencies.
    g. Collecting information about security incidents from LASOs for submission to the FBI.

B. Local Agency Security Officer (LASO)

1. Each agency head must appoint a LASO for the agency. The LASO, who is the liaison between his/her Local Agency and the CSA ISO, is responsible for ensuring that the agency complies with both the CSP and this policy.
2. The tasks assigned to the LASO in the CSP are modified as follows:
    a. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
    b. Identify and document how the equipment is connected to the state system.

c. Ensure that personnel security screening procedures are being followed as stated in the CSP ***in coordination with the agency's Terminal Agency Coordinator (TAC) or Point of Contact (POC).***
d. Ensure the approved and appropriate security measures are in place and working as expected.
e. Support policy compliance and keep the state/federal ISO informed of security incidents.
f. Ensure the physical security of all MNJIS terminals and equipment in the authorized agency's environment that accesses the CJDN or contains CJI.

C. Authorized Agency

The authorized agency using the CJDN is responsible for ensuring that personnel screening is conducted as required by the CSP and Minnesota Statutes, section 299C.46 and that users receive initial security awareness training and on-going security awareness training as outlined in the CSP.

D. Standards of Enforcement

1. Each Local Agency is responsible for enforcing system security standards for their agency in addition to all of the other agencies and entities which the Local Agency provides CJI services. Local Agencies must have written policies to address the security provisions of the CSP and this policy. Local Agencies must also have procedures in place to deactivate the passwords, log-ons, and other access tools of separated employees.
2. Authorized users must access CJIS systems and disseminate CJI only for the purposes for which they are authorized. Each authorized agency permitted access to FBI CJIS and Minnesota systems will be held to the provisions of the policies and guidelines set forth in this policy as well as the most current version of the CSP.

E. Personnel Security

1. According to the CSP, any individual with unescorted access in a Physically Secure Location must have a national, fingerprint-based background check and complete appropriate security awareness training. Most individuals will take the security awareness training via the BCA's Launch Pad (https://bcanextest.x.state.mn.us/launchpad/) by using the CJIS Online functionality. Access to these sites is restricted; access is granted by the TAC. As part of the training, individuals will be tested as required by the CSO. Each agency is responsible for keeping documentation of each employee's completion of security awareness training.
2. Once the individual has met the requirements, they can have unescorted access to any part of the Physically Secure Location where there are devices through which CJI can be accessed or where output from those devices can be found in any media (*e.g.* paper, electronic or other physical format).
3. Individuals who do not need to move freely within a Physically Secure Location must be escorted at all times by an individual who has met these Personnel Security requirements.
4. For individuals who have Occasional Unescorted Access within a Physically Secure Location, the security awareness training requirement is satisfied by signing an agreement acknowledging that they understand they are working in a location with access to protected data, whether access is via a device, printout or overheard conversation and that the protected data need to "remain in the building." The agreement must be signed prior to gaining access to CJI and must be renewed every two years. A sample agreement can be found on the BCA's CJDN Secure website, https://app.dps.mn.gov/cjdn/ under MNJIS Policies. Credentials for the CJDN Secure website are obtained from the BCA Service Desk (651-793-2500/ 1-888-234-1119 or bca.servicedesk@state.mn.us). The sample agreement can also be found on the BCA's Launch Pad in the CJIS Documents folder under the heading Security Awareness Training and Testing.

F. Personnel Screening for Contractors, Vendors, and Governmental Agencies Performing Criminal Justice functions on Behalf of an Authorized Agency

As provided in the CSP, the CSO sets the standard for background checks on contractors and vendors. The BCA will register companies whose employees support authorized agencies in Minnesota after determining that the company is in compliance with the CSP and has signed a

Security Addendum with the BCA. Part of the registration will include a determination that the 5050 company operates in compliance with the CSP and this policy. The BCA will conduct all national fingerprint-based background checks on all vendor employees and will be the centralized repository for the documentation of security awareness training and testing for those employees. Information on the process is available from the BCA CJIS SAT Screening Unit, *DPS_BCA CJIS SAT screening@state.mn.us.

G. Incident Response

1. The CSP requires that Local Agencies report a security incident, whether physical or logical, to the FBI via the CSA ISO. Local Agencies are required to have a policy regarding security incidents and how they are reported. Local Agencies should use NIST Special Publication 800-61 as a template for the required incident response policy. The NIST publication can be found at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
2. The Local Agency must report all suspected security incidents to the CSA ISO within 24 hours of the initial discovery. Security incidents include loss or theft of media containing CJI (e.g. paper, thumb drive) or equipment, suspicious or malicious software in the Local Agency's environment or unusual network activity. Information security events and weaknesses associated with information systems must be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and procedures to increase attention depending on the severity of the situation must be in place.
3. Wherever feasible, the Local Agency must employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users must be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

H. Firewalls

Local Agencies with access to a foreign network connected to the CJDN must be protected with a firewall device. This must include all forms of access including wireless, dial-in, off-site, Internet access, and others. Firewall architectures must prevent unauthorized access to CJI, the Local Agency's network, and all network components.

I. Advanced Authentication and Encryption

1. The technical security requirements for encryption and advanced authentication for CJI transmitted across the CJDN are as follows:
    a. Physically Secure Location with direct access to CJDN.
        i. Must use NIST-certified 140-2 encryption algorithm with a minimum of a128 bit encryption key.
        ii. No advanced authentication is required.
    b. Physically Secure Location to Physically Secure Location to CJDN. For example, a city police department has a network connection to the county sheriff's office which has direct access to CJDN.
        i. Must use NIST-certified 140-2 encryption algorithm with a minimum of a 128-bit encryption key.
        ii. No advanced authentication required.
2. Access to CJDN from a location that is not physically secure must use advanced authentication and encryption. Police vehicles in Minnesota are physically secure and so advanced authentication and encryption is not required.

J. Physically Secure Location

1. A Physically Secure Location is a facility, an area, a room, or a group of rooms, that is/are subject to authorized agency management control and which contain hardware, software, and/or firmware (*e.g.*, information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, *etc*.) that provide access to the CJIS and CJDN networks. Physical security perimeters must be acceptable to the CSO.

2. Restricted and controlled areas must be prominently posted and separated from non-physically secured areas by physical barriers that restrict unauthorized access. Every physical access point to physically secure areas housing information systems that access, process, or display CJI must be secured in a manner which is acceptable to the CSO during both working and non-working hours. ***In commercial buildings where the public has complete access to the building, the requirement of a physically secure location is met by a secured room within a secured room.***
3. All CJI transmitted through any public network segment or over Internet connections must be immediately protected using a NIST certified, FIPS 140-2 encryption algorithm using a minimum of a 128-bit encryption key. **This requirement also applies to any private data circuit.**
4. Advanced Authentication (AA) is the term describing added security functionality, in addition to the typical user identification and authentication of login ID and password, such as:
    a. Biometric systems
    b. Public Key Infrastructure (PKI)
    c. Smart cards
    d. Software tokens or hardware tokens
    e. "Risk-based Authentication" that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (*i.e.* device forensics, user pattern analysis and user binding) and user profiling, and also includes high-risk challenge/response questions.
5. The objectives of implementing AA are to uniquely and positively identify an authorized individual for access to CJI.
6. Once authenticated, access to CJI must be though a NIST certified, FIPS 140-2 encryption algorithm using a minimum of a 128-bit encryption key.
7. Encryption keys, such as pre-shared keys used in a site-to-site VPN, must be changed at least once a year.
8. Digital certificates, whether device and/or user based, must expire and be reissued at least once every two years.
9. AA does not have to be a part of establishing the encrypted transport.
10. No remote access to CJI, from an unsecure location, is permitted unless both AA and compliant encrypted transport requirements are met.
11. The infrastructure for AA/encryption must be on an isolated network, not part of the CJDN or a city/county user network.
12. The infrastructure for encryption must isolate authorized agency users from non-authorized agency users.
13. The agency must have a firewall between the CJDN and AA/encryption environments.
14. The agency firewall must ensure that only properly authorized and authenticated users may pass through the firewall to access CJI and/or any resources where CJI is in transit or at rest.
15. The agency AA/encryption environment may provide access to other non-criminal justice resources such as email and county/city resources as required.
16. Any agency AA methodology must utilize real-time user authentication to an agency controlled remote environment. Device authentication and locally cached credentials must not be used as part of AA.

K. Mobile Devices

The use of mobile devices to access CJI is rapidly changing and the FBI periodically issues additional direction on their use. Contact the CSA ISO for the most current requirements governing the use of these devices. The CSA ISO can be reached at bca.iso@state.mn.us.

L. Software as a Service (SaaS)

1. For an Authorized agency who wants to use a private sector vendor to provide SaaS the requirements are:
    a. An Authorized agency must consult with the BCA to ensure all requirements can be or are being met.
    b. The Authorized agency must send a written request, on agency letterhead, to the CSO requesting that vendor provide SaaS.
    c. The Authorized agency must have appropriate agreements in place with BCA.

d. The Authorized agency must have written contract with the vendor. The vendor must comply with the CSP and this policy as well as any contractors of Vendor.
    i. If the vendor is in the private sector, the Security Addendum needs to be signed and employees must sign Security Addendum Certification. If the vendor has subcontractors, there must also be a written agreement between them, along with Security Addendum and Security Addendum Certifications.
    ii. If the vendor is a non-criminal justice government agency, a Management Control Agreement is needed.
e. SaaS must be provided in an isolated network that must reside in the continental United States.
f. Data must be encrypted in transmission and at rest.
g. SaaS must be configured so that any agency may only have access to another criminal justice agency's data if the access is authorized by Minnesota law and the parties have a signed agreement approving the access.
h. Back up security must meet FBI CJIS requirements.
i. BCA must have access for audit.
j. Vendor/agency responsible for cost of connecting to the vendor, however accomplished.

M. Cloud Computing

1. Any authorized agency that wants to store CJI in or transmit CJI through a cloud environment **should consult** with the BCA prior to any storage or transmission of CJI. The BCA will reference the most current version of the FBI's Technical Report entitled "Recommendations for Implementation of Cloud Computing Solutions." (As of April 2017, the report was available at https://www.fbi.gov/file-repository/cjis-cloud-computing-report_20121214.pdf/view).
2. ***Any cloud implementation must host and/or access CJI separately from non-CJI.***

N. Electronic Media Disposal

When it is necessary to sanitize or destroy physical media, the use of media sanitization and destruction methods consistent with the applicable guidance contained in NIST 800-88 (available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf) and/or DOD 5220.22-M (available at http://www.dtic.mil/whs/directives/corres/pdf/522022M.pdf) is required.

O. Analytics Tools

Any Local Agency that wishes to use an analytic tool should consult with BCA prior to implementation to ensure that the tool is in compliance with the CSP and this policy.

P. Network Configuration

The LASO is responsible for ensuring network compliance with the CSP and establishing procedures for documenting, maintaining, and updating their agency's criminal justice information network configuration. Contact the CSO ISO at bca.iso@state.mn.us for assistance with network configurations.

References:

1. FBI CJIS Security Policy
2. NIST Special Publication 800-61
3. FBI Recommendations for Implementation of Cloud Computing Solutions
4. NIST 800-88
5. DoD 5220.22-M