CJDN Security

Version: 07/21/2023	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 and submit criminal justice information (CJI) to BCA systems and services to perform their duties.

This policy sets statewide standards regarding the security and movement of CJI within Minnesota, including security of the CJDN by providing specific guidance for meeting FBI *CJIS Security Policy* (CJISSECPOL) requirements. The CJIS Security Policy 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.

Any security controls listed in this policy that are more restrictive than the CJIS Security Policy are noted in ***bold and italics.*** These controls are detailed in the BCA CJDN Security Policy – Directive.

Definitions:

Authorized agency: A government entity authorized by statute to access BCA and FBI resources with a valid joint powers agreement or other contract executed by it and the BCA. Used interchangeably with Local Agency.

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

CJI Environment (CJE): an authorized agency's isolated infrastructure where CJI is processed, stored, or transmitted and access to environments is controlled. This includes, but is not limited to, network switches, routers, firewalls, workstations, mobile devices, servers, virtual environments. This also includes hosted, cloud-based delivery models such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Criminal Justice Information (CJI): Criminal Justice Information means all FBI CJIS-provided data necessary for authorized agencies to perform their duties, including data contained in, or derived from, data maintained by the BCA that have restricted dissemination standards under state or federal statute. BCA systems that frequently contain or provide CJI include PortalXL, Law Enforcement Message Switch (LEMS), the Criminal History System (CHS), Predatory Offender Registry (POR) System, and other systems listed in the BCA Data Inventory.

Criminal Justice Data Communications Network (CJDN): For statutorily authorized users, the CJDN is a connectivity method approved by the BCA and defined in *Minnesota Statute 299C.46*

Local Agency: A Minnesota government entity authorized by statute to access BCA and FBI resources with a valid joint powers agreement or other contract executed by it and the BCA. Used interchangeably with Authorized Agency.

Local Agency Point of Contact (POC): This is for non-criminal justice agencies only. The POC administers CJIS systems programs within the local organization and oversees the organization's compliance with CJIS systems policies. Additionally, the POC is knowledgeable in all aspects of the organization's retrieval, dissemination, storage and destruction of CHRI.

Local Agency Terminal Agency Coordinator (TAC): The point of contact at the Local Agency for matters relating to CJIS and BCA information access. The TAC administers CJIS and BCA systems programs within the Local Agency and oversees agency compliance with the FBI CJIS Security Policy, NCIC Operating Manual, BCA CJDN Security Policy, BCA Appropriate Use of Systems and Data policy, BCA FBI CJIS Audits, Audit Compliance, Audit Sanctions policy, and other FBI and BCA policies.

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.

Physically Secure Location: 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, firmware, and hard copy Criminal Justice Information (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels) that provide access to the CJDN or the CJE. Physical security perimeters must be acceptable to the state CJIS Systems Officer (CSO).

Policy:

This policy addresses the secure operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that support a data network, telecommunications network and related MNJIS systems used to process, store, share, or transmit CJI, guaranteeing the priority, integrity, availability, and security 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)

The CSA ISO is a BCA employee who, in addition to the responsibilities described in the CJIS Security Policy, is responsible for:

1. Ensuring agencies conform to the CJIS Security Policy and BCA policies related to the security and compliance of systems and connections to the CJDN and/or the access, transmission, or processing of CJI.
2. Ensuring management controls are in place for the CJDN, including the management of state routers, firewalls, and VPN devices.
3. Ensuring that state and Local Agency network topology documentation is current.
4. Supporting security-related configuration management for the BCA and local agencies.
5. Disseminating security-related training materials to local agencies.
6. Ensuring the completion of technical security compliance audits for all agencies who access the CJDN and/or CJI.

B. Local Agency Security Officer (LASO)

Each head of a Local Agency, whether criminal justice or non-criminal justice, that accesses CJI, must appoint a Local Agency Security Officer (LASO) for the agency. The LASO is the liaison between the Local Agency and the CSA ISO. The LASO is responsible for ensuring that the agency complies with the CJIS Security Policy, this policy, and the CJDN Security Policy Standards Directive. In addition to responsibilities outlined in the CJIS Security Policy, the LASO is responsible for:

1. Ensuring that personnel security screening procedures are being followed as stated in the CJISSECPOL in coordination with the agency's Terminal Agency Coordinator (TAC) or Point of Contact (POC).
2. Ensuring the physical security of all terminals and equipment in the authorized agency's environment that access the CJDN or process, store, share, or transmit CJI
3. Ensuring network compliance with the CJIS Security Policy.
4. Establishing procedures for documenting, maintaining, and updating their agency's criminal justice information network configuration and required policies.

C. Standards of Enforcement

1. Each Local Agency is responsible for enforcing system security standards and incident response procedures for their agency in addition to any other agencies or entities for which the Local Agency provides CJI data or services.
2. Local Agencies must have written policies to address the security provisions of the CJISSECPOL and this policy. Local agencies must have procedures in place to deactivate the accounts, passwords, and other access tools of separated employees.
3. Authorized users may access CJIS systems and disseminate CJI only for the purposes for which they are authorized. Each authorized agency permitted access to FBI CJIS and BCA systems will be held to the guidelines set forth in this policy, as well as the most current version of the CJIS Security Policy.

D. Personnel Security

1. The CJIS Security Policy requires any individual with unescorted access in a physically secure location to have a national, fingerprint-based background check and complete the required level of Awareness and Training depending on their role. Most individuals will take the Awareness and Training via the BCA's Launch Pad (https://bcanextest.x.state.mn.us/launchpad/). Access to these sites is restricted; access is granted by the TAC or POC. As part of the training, individuals will be tested as required by the CJISSECPOL. Each agency is responsible for ensuring each employee is current with Awareness and Training.
2. Once the individual has met the requirements, they are allowed unescorted access to any part of the agency's 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.

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

As an alternative to agencies screening vendors themselves, the BCA offers an optional Vendor Screening Program to register private vendors whose employees support authorized agencies in Minnesota. Vendors will be registered after the BCA determines the vendor is acting in compliance with the CJISSECPOL and this policy, the vendor's product(s) or services(s) being screened are capable of being implemented or provided in compliance with the CJISSECPOL and this policy, commits to maintaining compliance, and has signed a Security Addendum with the BCA. For vendors who participate in this program, the BCA will conduct all national fingerprint-based background checks on vendor employees who may have access to CJI, and will be the centralized repository for the documentation of Awareness and Training and testing for those employees. Information on the process is available from the BCA CJIS SAT Screening Unit, BCACJISSATScreening@state.mn.us

F. Incident Response

1. The CJIS Security Policy requires that local agencies report a computer security incident, whether physical or logical, to the FBI via the CSA ISO. Local agencies are required to have a policy and procedure regarding computer 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 initial discovery. Computer security incidents include loss or theft of media containing CJI (e.g. paper, thumb drive), suspicious or malicious software in the Local Agency's environment, or unusual network activity. Computer 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 escalation procedures, depending on the severity of the situation, must be in place.

3. All employees, contractors and third party users must be made aware of the procedures for reporting different types of events and weaknesses that may have an impact on the security of agency assets; all are required to report any computer security events and weaknesses as quickly as possible to the designated point of contact.

Technical Security Standards

Local agencies must follow the technical security standards found in the CJIS Security Policy Standards Directive for their agency and any other agencies or entities for which the Local Agency provides CJI data or services.

References:

1. FBI CJIS Security Policy
2. NIST Computer Security Incident Handling Guide Special Publication 800-61 Rev. 2
3. NIST Cloud Computing Synopsis and Recommendations Publication 800-146
4. NIST Guidelines for Media Sanitization Special Publication 800-88
5. FBI Recommendations for Implementation of Cloud Computing
6. FBI Cloud Control Catalog

CJDN Security Policy Standards Directive

SECTION 1 – INTRODUCTION

1.1 Purpose

As the CJIS Systems Agency (CSA) for the State of Minnesota, the Bureau of Criminal Apprehension (BCA) is responsible for ensuring that all criminal justice and non-criminal justice agencies in Minnesota that access criminal justice information (CJI) comply with FBI CJIS Security Policy requirements.

The FBI CJIS Security Policy (CJISSECPOL) provides agencies with a minimum set of security requirements for access to FBI Criminal Justice Information Services (CJIS) systems and information. As a supplement to the FBI CJIS Security Policy, the BCA has developed this directives document to clarify FBI requirements and provide additional standards for the protection of criminal justice information and systems in the state.

This directive will be reviewed and updated as necessary at least every six months.

SECTION 2 – POLICIES

2.1 Logging[1]

1. All user and administrative account active logons, logoffs, and events related to access to criminal justice information must be logged and reviewed weekly for anomalies.
2. All computer systems (e.g., servers, desktops, laptops, smartphones), network equipment, and cloud environments where CJI is accessed, transmitted, processed, or stored must be logged and reviewed weekly for anomalies.
3. Logs must be maintained for one year.

2.2 Advanced Authentication[2]

1. Access to the CJDN from a location that is not physically secure must use advanced authentication and encryption.
2. The infrastructure for advanced authentication must be on an isolated network, not part of the CJDN or an agency user network.
3. Biometrics may not be used as a second factor of authentication on mobile devices.
4. CJI access in a cloud environment must use a government cloud, as well as advanced authentication and encryption.

2.3 Encryption[3]

1. All compromised or weak methods of communication must be disabled. Only cryptographic methods that have no known compromises may be used.
    a. The following cipher suite modes must be disabled: RSA, AES-CBC, SHA, MD5, EDH, DHE, null, DES, 3DES, RC4, and EXPORT-Strength Ciphers.
    b. Only supported TLS protocols may be used - TLS 1.2 or TLS 1.3 with non-compromised ciphers/authentication only.
2. Encryption devices must be operated in FIPS mode. This removes support for most weak or compromised protocols.
3. Encryption keys, such as pre-shared keys in a site-to-site VPN, must be changed at least annually.
4. Digital certificates, whether device- or user-based, must expire and be reissued at least once every two years.
5. Encryption infrastructure must be on an isolated network (i.e., not part of the CJDN or an agency user network).

2.4 Firewalls[4]

1. Agencies must employ firewall technology to separate their CJDN network(s) from non-CJDN network(s).
2. Firewall architectures and configurations must prevent unauthorized access to the CJDN and CJI.
3. Firewall equipment must be operated in FIPS mode.

[1] FBI CJIS Security Policy Section 4.2.5.1, 5.4.1.1, 5.4.1.1.1, 5.10.1.3, and 5.13.1.1, and Appendices D.1 and G.1
[2] FBI CJIS Security Policy Section 5.5.6, 5.6, and 5.13.7.2
[3] FBI CJIS Security Policy Section 5.10.1.2.1
[4] FBI CJIS Security Policy Section 5.10.1.2.1

2.5 Cloud

2.5.1 Cloud Security[5]

1. Storage of CJI, regardless of encryption status, is permitted only in government cloud environments which reside within:
    a. the physical boundaries of the U.S., U.S. territories, Indian Tribes, and Canada, and
    b. the legal authority of an FBI Advisory Policy Board (APB) member agency (i.e., U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).
2. Any cloud vendor employees with access to unencrypted CJI or encryption keys for encrypted CJI must:
    a. reside within the U.S., U.S. Territory, Indian Tribe, or Canada, and
    b. perform all work from the same.
3. Encryption keys should be managed by the agency and must be rotated at least yearly.
4. If encryption keys cannot be managed by the agency, the agency's vendor agreement must limit vendor employee access to keys and specify related vendor responsibilities.

2.6 Faxing (Digital)[6]

1. When using a digital fax machine that uses the agency network and the Internet to transmit the files, NIST-certified FIPS 140-2 compliant encryption with a 128-bit symmetric key is required.

2.7 Virtualization[7]

1. The following controls must be implemented in any virtual environment that contains CJI:
    a. The host must be isolated from the virtual machine so virtual machines cannot access host files, firmware, etc.
    b. Audit logs must be maintained for all virtual machines and hosts for one year.
    c. Audit logs must be stored outside the host's virtual environment.
    d. Virtual machines that are Internet-facing (e.g., web servers, portal servers) must be separate from virtual machines that process CJI internally or be separated by a virtual firewall.
    e. Drivers that serve critical functions must be stored within the specific virtual machine they service. They may not be stored within the hypervisor or host operating system for sharing.
    f. Each virtual machine must be treated as an independent system, secured as independently as possible.
2. The following additional technical security controls must be followed where CJI is commingled with other data:
    a. Encrypt data at rest using FIPS 197 compliant AES encryption with a minimum 256-bit symmetric key.
    b. Encrypt network traffic within the virtual environment using FIPS 140-2 compliant encryption with a minimum 128-bit symmetric key.
    c. Implement intrusion detection and/or intrusion prevention (IDS and/or IPS) within the virtual environment.
    d. Virtually or physically firewall each virtual machine within the virtual environment to ensure that only allowed protocols will transact.
    e. Segregate the administrative duties for the host.

[5] FBI CJIS Security Policy Section 5.10.1.5 and Appendix G.3
[6] FBI CJIS Security Policy Section 5.10.2
[7] FBI CJIS Security Policy Section 5.10.3.2

2.8 Personnel Security[8]

1. The Agency TAC is able to make approval decisions for background checks according to the "Designation of Individuals Authorized to Approve Access to Criminal Justice Information under FBI CJIS Security Policy" located in the BCA's Launch Pad (https://bcanextest.x.state.mn.us/launchpad/).

2.9 Radio Traffic[9]

1. Radio traffic containing CJI must be encrypted using NIST-certified FIPS 140-2 compliant encryption with a 128-bit symmetric key.
2. 911 and dispatch radio calls containing CJI in a cloud environment or outside of a physically secure environment must be encrypted at rest using FIPS 197 AES encryption with at least a 256-bit symmetric key.

2.10 Account Administration

2.10.1 User Accounts

1. Agency must have a documented process for validating user identities before unlocking any accounts that may provide access to CJI.
2. User credentials used to access CJI must be protected as CJI, even though they are not themselves CJI.

2.10.2 Network and Service Accounts[10]

1. Network and Service Account passwords shall be a minimum of twenty (20) characters in length including at least one of each of the following:
    a. special character
    b. number
    c. upper case character
    d. lower case character
2. If the agency uses a Privileged Account Management (PAM) tool, these accounts shall be managed using the tool and changed at minimum every 90 days.
3. If the agency does not use a PAM tool, a documented process must be used to manage these accounts and the passwords will be changed at minimum every 6 months.

2.11 Application Development

2.11.1 Application and Application Programming Interface (API) Coding[11]

1. Agencies must implement the practices in FBI CJIS Security Policy Appendix G.8 and as outlined below when developing any applications or application integrations that access, transmit, process, or store CJI. These practices must be followed by all agency staff, including employees and contractors, involved in application architecture, design, develop, or testing.
2. Security Controls: Using a set of standard security controls greatly simplifies the development of secure applications and APIs. The OWASP Top Ten Proactive Controls 2018 is a list of security techniques that should be included in every software development project. They are numbered in order of importance (i.e., #1 being most important):

[8] FBI CJIS Security Policy Section 5.12.1
[9] FBI CJIS Security Policy Section 5.13.1
[10] FBI CJIS Security Policy Appendix G.5
[11] FBI CJIS Security Policy Appendix G.8

a. C1: Define Security Requirements
b. C2: Leverage Security Frameworks and Libraries
c. C3: Secure Database Access
d. C4: Encode and Escape Data
e. C5: Validate All Inputs
f. C6: Implement Digital Identity
g. C7: Enforce Access Controls
h. C8: Protect Data Everywhere
i. C9: Implement Security Logging and Monitoring
j. C10: Handle All Errors and Exceptions

3. For more details see:
    a. https://www.owasp.org/index.php/OWASP_Proactive_Controls
    b. https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series

2.11.2 Application Logging

1. Custom-developed applications must log the following events:
    a. Input validation failures (e.g., protocol violations, unacceptable encodings, invalid parameter names and values)
    b. Output validation failures (e.g., database record set mismatch, invalid data encoding)
    c. Authentication successes and failures
    d. Authorization (access control) failures
    e. Session management failures (e.g., cookie session identification value modification)
    f. Application errors and system events (e.g., syntax and runtime errors, connectivity problems, performance issues, third party service error messages, file system errors, file upload virus detection, configuration changes)
    g. Application and related system start-ups and shut-downs
    h. Logging initialization (starting, stopping or pausing)
    i. Use of higher-risk functionality, such as:
        i. network connections
        ii. addition or deletion of users
        iii. changes to privileges
        iv. assigning users to tokens
        v. adding or deleting tokens
        vi. use of systems administrative privileges
        vii. access by application administrators
        viii. all actions by users with administrative privileges
        ix. access to payment cardholder data or criminal justice data
        x. use of data encrypting keys
        xi. encryption key changes
        xii. creation and deletion of system-level objects
        xiii. data import and export (including screen-based reports)
        xiv. submission of user-generated content – especially file uploads
    j. Legal and other opt-ins, such as:
        i. permissions for mobile phone capabilities
        ii. terms of use
        iii. terms and conditions
        iv. personal data usage consent
2. All application logs must be stored for one year.

3. All application logs must be reviewed weekly for anomalies. Automated anomaly review using a security information and event management (SIEM) tool may substitute for the manual weekly review.
4. Each log entry must include sufficient detail to identify "when, where, who, and what" for each event. For more detail, reference the OWASP Logging Cheat Sheet below.
   https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

2.11.3 Application Code Scanning

2.11.3.1 Static Application Security Testing (SAST)

1. SAST analyzes source code without executing the application to identify any vulnerabilities.
   a. SAST must be performed on any custom-built applications that will access, transmit, process, or store CJI before the application is deployed to production and during any major updates or upgrades.
   b. SAST tools used by the agency should identify severity ratings for vulnerabilities using the Common Vulnerability Scoring System (CVSS).

2.11.3.2 Software Composition Analysis Testing (SCA)

1. SCA scans an application's direct and transitive dependencies for security vulnerabilities.
   a. SCA must be performed on any custom-built applications that will access, transmit, process, or store CJI before the application is deployed to production and during any major updates or upgrades.
   b. SCA tools used by the agency should identify severity ratings for vulnerabilities using the CVSS.

2.11.3.3 Dynamic Application Security Testing (DAST)

1. DAST tests an application when it is running to discover run-time and environment-related security issues.
   a. DAST must be performed on all applications, custom-developed and commercial off-the-shelf (COTS), before the application is placed into production and during any major updates or upgrades.
   b. DAST tools used by the agency should identify severity ratings for vulnerabilities using the CVSS.

2.11.4 Application Code Vulnerability Remediation

1. Agencies and their vendors must use the standards outlined below to remediate any vulnerabilities identified during code scanning for both custom-developed and COTS applications that access, transmit, process, or store CJI.
2. Using the CJIS Security Policy (CJISSECPOL) and Common Vulnerability Scoring System (CVSS), agencies and their vendors must remediate vulnerabilities as follows:
   a. **Critical – Remediate within 7 days.** These vulnerabilities pose the highest risk to applications, systems, and agency data.
   b. **High – Remediate within 30 days.** These vulnerabilities pose a significant risk to applications, systems, and agency data.
   c. **Medium– Remediate within 60 days.** These vulnerabilities pose a moderate to indirect risk to applications, systems, and agency data.
   d. **Low – Remediate within 90 days.** These vulnerabilities only expose non-critical system information.

2.12 BCA Systems and Data Access

1. BCA systems and data may be accessed via:
   a. the BCA's Criminal Justice Data Communications Network (CJDN), or
   b. a VPN connection that meets the FBI CJIS Security Policy and BCA CJDN Security Policy requirements for encryption of data in transit, including disabling all compromised cipher suites, and operating devices in FIPS Mode.

2.13 Camera Guidance (Body, Squad, Surveillance, Drone)

1. Video files are not considered criminal justice information. Any CJI captured in these files is considered incidental. Neither the FBI nor BCA has requirements related to cameras or video files.
2. MN Statutes §13.825 subd. 11(b) requires portable recording system vendors storing data in the cloud to "protect the data in accordance with the security requirements of the United States Federal Bureau of Investigation Criminal Justice Information Services Division Security Policy 5.4 or its successor version."

2.14 Conferencing (Audio, Video)

1. Audio and video conferencing systems used for transmitting or storing CJI must comply with all FBI CJIS Security Policy and CJDN Security Policy requirements for encryption at rest and in transit.

2.15 Employees, Vendors, and Contractors

1. Agency will not hire or contract with any person not physically present within an APB-member country for work related to any system that will access, transmit, process, or store CJI.
2. Any employee, contractor, or vendor employee must:
    a. be a resident of an APB-member country, and
    b. submit to a fingerprint-based state of residence and national fingerprint check with no disqualifying responses.

2.16 File Transfers

1. All file transfers to or from the CJDN must use Secure File Transfer Protocol (SFTP).

2.17 Wireless Networks

1. When any wireless network is used to transmit CJI, a VPN connection is required.

2.18 Cellular Devices

1. SIM Swapping is not allowed for devices that process, store, or transmit CJI.
2. Air Drop is not allowed for devices that process, store, or transmit CJI.

2.19 Mobile Device Management (MDM)

1. Cloud-based Mobile Device Management must use a government cloud for devices that access, transmit, process, or store CJI.

2.20 Multifunction Devices and Printers

1. Printers and multifunction devices must be configured securely, with least function and least privilege.
2. Printer hard drives must be disposed of or sanitized in compliance with CJIS Security Policy requirements.
3. Printing of CJI is not allowed over a wireless home network.

2.21 Soft Phones

1. If CJI will be discussed using soft phones, all CJIS Security Policy and CJDN Security Policy requirements related to encryption in transit and at rest must be followed.
2. Soft phone traffic traversing a VPN must be encrypted using a different encryption key than the VPN uses.

2.22 Virtual Private Network (VPN)

1. For any user VPN connection, a network disconnect must be executed after 12 hours, regardless of whether data is being transmitted.
2. VPN is required when any wireless network is used to transmit CJI.

2.23 Vulnerability Remediation and System Updates

1. All systems, infrastructure, workstations, mobile devices, network equipment, etc., must be regularly updated to prevent or resolve system vulnerabilities in alignment with the CJIS Security Policy (CJISSECPOL) and the Common Vulnerability Scoring System (CVSS):
    a. **Critical – Remediate within 7 days *(CVSS)*.** These vulnerabilities pose the highest risk to applications, systems, and agency data.
    b. **High – Remediate within 30 days *(CJISSECPOL and CVSS)*.** These vulnerabilities pose a significant risk to applications, systems, and agency data.
    c. **Medium– Remediate within 60 days *(CJISSECPOL)*.** These vulnerabilities pose a moderate to indirect risk to applications, systems, and agency data.
    d. **Low – Remediate within 90 days *(CJISSECPOL)*.** These vulnerabilities only expose non-critical system information.

APPENDIX A – SUPPORTING INFORMATION FOR CLOUD SERVICES

If CJI will be processed, stored, or transmitted, the cloud service must be in a government cloud. FBI CJIS Security Policy section 5.10.1.5 requires that "the storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial data centers, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of APB-member (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP))."

This section also states that any metadata derived from unencrypted CJI must be protected in the same manner and may not be used for any commercial purpose by a cloud provider or other associated entity.

A government cloud such as Microsoft Azure Government Cloud or AWS Government Cloud can meet CJIS Requirements if configured correctly. It is your agency's responsibility to ensure a compliant configuration.

Ensuring Cloud Vendor Security and Compliance with the FBI CJIS Security Policy
Agencies must review a vendor's security practices for any services they provide, including any cloud services used in providing those services. The FBI CJIS Security Policy requires:

- vendors sign a CJIS Security Addendum as part of their contract with agencies, and
- any vendor employees who will have access to unencrypted CJI must complete fingerprint-based background checks and the appropriate level of CJIS Awareness and Training.

As an optional service to agencies, the BCA maintains a Vendor Screening Program that can complete the vendor security and compliance review. The BCA would then enter into a contract with the vendor (including the vendor's signed CJIS Security Addendum). It would also oversee background checks and training for any vendor employees with access to unencrypted CJI.

- More information about the BCA Vendor Screening Program can be found at https://dps.mn.gov/divisions/bca/bca-divisions/mnjis/Pages/bca-vendor-screening-program.aspx
- Agencies or vendors who would like to use this program can contact the Vendor Screening Program at BCACJISSATScreening@state.mn.us

Agency Responsibility for Ensuring Security and Compliance
Regardless of who screens the vendor, your agency is responsible for ensuring the security and FBI CJIS Security Policy compliance of any cloud service(s) it uses. Vendor screening determines whether they are capable of meeting and agreeing to meet FBI CJIS Security Policy requirements. This does not guarantee compliance.

Each agency that uses cloud services must:

- ensure their implementation meets FBI CJIS Security Policy requirements,
- ensure controls are in place to ensure ongoing compliance, and
- review compliance on an ongoing basis.

Microsoft Cloud Services
The BCA entered into a statewide five-year contract with Microsoft for its Office 365 and Azure Government Cloud services in January 2016 and is renewing its agreement through 2026. As part of the agreement, the BCA ensures that any Microsoft employees who will have access to unencrypted CJI complete the appropriate background check and CJIS Awareness and Training. Individual agencies must ensure that they only use Microsoft Government Cloud services for CJI and that their use of any Microsoft Government Cloud services meets FBI CJIS Security Policy requirements.

Amazon Web Services (AWS)

The BCA entered into a similar statewide five-year contract with Amazon in February 2016. Rather than establishing statewide agreements, AWS will work with individual agencies and vendors to ensure that their AWS Government Cloud implementations use FBI CJIS Security Policy compliant encryption and encryption key management to protect CJI at rest and in transmission. By doing this, no AWS employees have access to unencrypted CJI, meaning that the CJIS Security Addendum and vendor employee background checks will not be required.

AWS GovCloud (U.S.) supports compliance with United States International Traffic in Arms Regulations (ITAR). As a part of managing a comprehensive ITAR compliance program, companies that are subject to ITAR export regulations must control unintended exports by restricting access to protected data to US Persons, and by restricting the physical location of protected data to the US. AWS GovCloud (US) provides an environment that is physically located in the US, and access by AWS personnel is limited to US Persons, thereby allowing qualified companies to use AWS to transmit, process, and store protected articles and data subject to ITAR restrictions. The AWS GovCloud (US) environment has been audited by an independent third-party assessment organization (3PAO) to validate that proper controls are in place to support customer export compliance programs.

- AWS Compliance Program – ITAR https://aws.amazon.com/compliance/itar/
- AWS Compliance Program – CJIS Security Policy: https://aws.amazon.com/compliance/programs/

Cloud Networking – Cisco Meraki

Things to consider when implementing Meraki:

- The MX product suite is cloud-managed. Disabling Meraki personnel access to dashboards, etc., should be considered to prevent unwanted access to agency data. This is done inside of the dashboard configuration. After completion, verify that Meraki personnel do not have access to any agency data unless specifically authorized.
- Refer to the Cloud Security subsection for additional guidance related to data storage and encryption.
- Enable Syslog and NetFlow capabilities within the Meraki device. The default functionality is limited.
- Ensure there is no loss of intrusion detection/prevention capabilities when switching products. Meraki offers various tools that can perform these functions. Those tools may have an additional cost.