CJIS-CT Information Security Policy

(Applicable to Connecticut Criminal Justice Information Systems managed by CJIS-CT)

Version 2.0
July 24, 2025

Approved by
CJIS-CT Governing Board

CT Criminal Justice Information System (CJIS-CT)
11th Floor, 55 Farmington Avenue
Hartford, CT 06105-3725

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
2.0	Policy rewritten with updates and additions to reflect latest version of FBI CJIS security policy (version 6.0) and additional feedback provided by DAS/BITS CISO, DESPP COLLECT Unit, and Connecticut CSO office. See subsequent summary of changes.	CJIS-CT	7/24/2025	CJIS-CT Governing Board
1.0	Policy Written	CJIS-CT	10/16/2014	CJIS-CT Governing Board

Summary of Changes – Version 2.0

Sections Updated

1. 5.1-Information Exchange Agreements
2. 5.2-Access Control
3. 5.3-Awareness and Training
4. 5.4-Audit and Accountability
5. 5.6-Configuration Management
6. 5.8-Identification and Authentication
7. 5.9-Incident Response
8. 5.11-Media Protection
9. 5.12-Physical and Environmental Protection
10. 5.14-Personnel Security
11. 5.18-System and Information Integrity

Sections Added

1. 5.5-Assessment, Authorization, and Monitoring
2. 5.7-Contingency Planning
3. 5.10-Maintenance
4. 5.13-Planning
5. 5.15-Risk Assessment
6. 5.16-Systems and Service Acquisition
7. 5.17-System and Communications Protection
8. 5.19-Supply chain risk management
9. 5.20-Mobile Devices

Contents

Executive Summary

Law enforcement needs timely and secure access to services that provide data wherever and whenever needed for stopping and reducing crime. In response to these needs, the CJIS-CT Governing Board authorized the Criminal Justice Information System (CJIS-CT) to update and expand the existing security policy approved in 2014. Taking that direction, this Security Policy Committee has attempted to meet the vision of establishing a security policy that maintains appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the Connecticut Information Sharing System (CISS) State Data.

Administered through a shared management philosophy, the CJIS-CT Security Policy contains information security requirements, guidelines, and practices reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of CISS State and CJI Data. It includes agency self- assessment and certification tools designed to minimize the administrative burden on both CJIS-CT and the agencies.

The CJIS-CT Security Policy is meant to:

- Allow agencies access CISS State and CJI Data while providing appropriate controls to protect the full lifecycle of State Data
- Stand as a baseline policy and aligns with FBI CJIS Security Policy version 6.0, December 2024.
- Provide guidance for the viewing, transmission, dissemination, storage, and destruction of State Data and CJI Data
- Apply to every individual—contractor, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information
- This policy is a minimum standard security policy for accessing CISS Search only and does not restrict agencies from creating a more stringent security policy for their purposes.

The CJIS-CT Security Policy aligns with the latest version of FBI CJIS Security Policy and ensures that Connecticut's State Data and Criminal Justice Information (CJI) are protected under federal and state security mandates. This policy is periodically updated to meet the evolving security landscape and maintain compliance with FBI CJIS requirements.

The CJIS-CT Security Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. It empowers agencies with the insight and ability to tune their security programs according to their needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. It also provides a secure framework of standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and non-criminal justice communities.

The CJIS-CT Security Policy incorporates and aligns with the key principles and security controls outlined in the FBI CJIS Security Policy. Where applicable, essential controls from the FBI CJIS Security Policy have been explicitly replicated and made visible within this document to ensure consistency, compliance, and seamless implementation within our operational framework. This approach ensures that all standards, procedures, and controls are maintained in accordance with federal requirements while adapting them to our specific environment.

1. Introduction

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The purpose of this document is to protect and safeguard data and information that is available electronically during the criminal justice process as defined below, regardless of whether the data or information is less protected or available more readily through other mediums. This document provides a minimum set of security requirements within the FBI Security Policy to ensure continuity of information protection, for information both at rest and in transit. This policy is to supplement the FBI's policy.

The CJIS-CT Security Policy provides Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) with a minimum set of security requirements for access to Connecticut (CT) Criminal Justice Information System (CJIS-CT) and information and to protect and safeguard CT criminal justice information, CT non-criminal justice information and FBI data. This minimum standard of security ensures continuity of information protection. The essential premise of the CJIS-CT Security Policy is to provide the appropriate controls to protect CT criminal justice information and CT non-criminal justice information, from creation through dissemination, whether at rest or in transit.

1.2 Scope

By the authority vested in the Governing Board through **54-142q** sections through **54-142s** of the general statutes, the CJIS-CT Governing Board adopted the CISS Security Policy to establish a minimum set of security requirements that all agencies and authorized persons shall comply with to receive gateway access to CISS.

The CJIS-CT Security Policy supersedes and replaces any contradictory provisions of the security policies that were previously drafted or issued for Offender Based Tracking System (OBTS) and Connecticut Impaired Driver Records Information System (CIDRIS).

The CJIS-CT Security Policy does not supersede or replace the FBI CJIS Security Policy to the extent that the FBI CJIS Security Policy applies to CJIS-CT State Data.

1.3 Relationship with Local Security Policy and Other Policies

The CJIS-CT Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS-CT Security Policy with a FBI CJIS Security Policy, or the agency may develop their own stand-alone security policy; however, the CJIS-CT Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the FBI CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS-CT Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS-CT Security Policy areas can be developed for the security program in general, and for a particular information system, when required by the CJIS-CT Governing Board.

This document is a compendium of applicable policies in providing guidance on the minimum-security controls and requirements needed to access CJIS-CT information and services. State and local Agencies may implement more stringent policies and requirements.

1.4 Terminology Used in This Document

The following terms are used interchangeably throughout this document:

i. Agency and Organization: The two terms in this document refer to any entity that submits or receives information, by any means, to/from CJIS-CT, FBI CJIS systems or services.
ii. Information and Data: Both terms refer to State Data and CJI.
iii. System, Information System, Service, or named applications like NCIC: all refer to connections to the CJIS-CT systems and FBI's criminal justice information repositories and the equipment used to establish said connections.
iv. References/Citations/Directives: References used in this Policy are mentioned in the Appendix and may contain additional sources that could apply to any section.

1.5 Administration

The CJIS-CT Security Policy shall be amended or changed by the CJIS-CT Governing Board. The CJIS-CT Security Policy shall be revised annually and will follow the SOP established for review and approval of the CJIS-CT Security Policy.

1.6 Distribution of the CJIS-CT Security Policy

The CJIS-CT Security Policy, Version 2.0, is a publicly available document and may be posted and shared without restrictions.

2. The CJIS-CT Security Policy Approach

The CJIS-CT Security Policy represents the shared responsibility between CJIS-CT and agencies submitting data of the lawful use and appropriate protection of State Data, CJI and Non CJI. The FBI CJIS Security Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new CJIS-CT initiatives.

2.1 CJIS-CT Security Policy Vision Statement

The vision of the CJIS-CT Security Policy is to establish a security policy that maintains appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the State and FBI Data. The CJIS-CT Governing Board collaborates with CJIS-CT to ensure that the Policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

The CJIS-CT Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provides the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides CJIS-CT with the flexibility for tuning the information security infrastructure and policies to reflect their own environments within the compliance requirements of the FBI Security Policy.

2.3 Risk versus Realism

Every "shall" statement contained within the CJIS-CT Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS-CT Security Policy is to establish the security requirements in accordance with the FBI Security Policy.

3. Roles and Responsibilities

In the scope of information security, the CJIS-CT employs a shared management philosophy with state and local law enforcement agencies. Through the CJIS-CT Governing Board and its Subcommittees, consideration is given to the needs of the CJIS-CT community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS-CT systems and information. The CJIS-CT Governing Board represents state and local law enforcement and criminal justice agencies throughout the State of Connecticut.

3.1 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI and Non CJI between the CJIS-CT and its user community. This section provides a description of the following entities and roles:

- CJIS-CT Governing Board
- CJIS-CT Executive Director
- Terminal Agency Coordinator
- Criminal Justice Agency
- Noncriminal Justice Agency
- CJIS-CT Information Security Officer
- CISS Administrator
- Agency Security Officer
- CISS Community Agency Administrator

3.1.1 CJIS-CT Governing Board

The CJIS-CT Governing Board as defined under section 54-142q subsection (b) of the general statutes is as follows.

“There shall be a Criminal Justice Information System Governing Board which shall be within the Department of Emergency Services and Public Protection for administrative purposes only and shall oversee criminal justice information systems”

Also, in section 54-142q(f), “The CJIS-CT Governing Board shall develop plans, maintain policies and provide direction for the efficient operation and integration of criminal justice information systems, whether such systems service a single agency or multiple agencies. The governing board shall establish standards and procedures for use by agencies to assure the interoperability of such systems, authorized access to such systems and the security of such systems.”

3.1.2 CJIS-CT Executive Director

The CJIS-CT Executive Director is an individual designated by the CJIS-CT Governing Board as responsible for the administration of the CJIS-CT network for the State Data including where FBI data is transported or stored. The role of CJIS-CT Executive Director shall not be outsourced. The CJIS-CT Executive Director may delegate responsibilities to subordinate agencies.
The CJIS-CT Executive Director shall set, maintain, and enforce the following:

- Standards for the selection, supervision, and separation of personnel who have access to

CJI and Non CJI.

- Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS-CT systems used to process, store, or transmit CJI and Non CJI, guaranteeing priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
- Ensure appropriate use, enforce system discipline, and ensure CJIS-CT operating procedures are followed by all users of the respective services and information.
- Ensure state/local agency compliance with policies approved and adopted by the CJIS-CT Governing Board.
- Ensure the appointment of the CJIS Information Security Officer (ISO) and determine the extent of authority to the CJIS-CT ISO.
- The CJIS-CT Executive Director, or designee, shall ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS-CT systems.
- Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
- Approve access to CJIS-CT systems after reviewing CJIS-CT Forms 1 and 2.
- Assume ultimate responsibility for managing the security of CJIS-CT systems within their state and/or agency.
- Perform other related duties outlined by the user agreements with CJIS-CT.

3.1.3 Terminal Agency Coordinator (TAC)

The Terminal Agency Coordinator (TAC) serves as the point-of-contact at the agency for matters relating to CJIS-CT information access. The TAC administers CJIS-CT systems programs within the agency and oversees the agency's compliance with CJIS-CT systems policies.

3.1.4 Criminal Justice Agency (CJA)

Criminal justice agency (CJA) means any court with criminal jurisdiction, the Department of Motor Vehicles or any other governmental agency created by statute which is authorized by law and engages, in fact, as its principal function in activities constituting the administration of criminal justice, including, but not limited to, organized municipal police departments, the Division of State Police, the Department of Correction, the Court Support Services Division, the Office of Policy and Management, the state's attorneys, assistant state's attorneys and deputy assistant state's attorneys, the Board of Pardons and Paroles, the Chief Medical Examiner and the Office of the Victim Advocate. Criminal justice agency includes any component of a public, noncriminal justice agency if such component is created by statute and is authorized by law and, in fact, engages in activities constituting the administration of criminal justice as its principal function.

3.1.5 Noncriminal Justice Agency (NCJA)

A noncriminal justice agency (NCJA) is defined (for the purposes of access to CJI and Non CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.1.6 CJIS-CT Information Security Officer (ISO)

The CJIS-CT Information Security Officer (ISO) shall:

- Document technical compliance with the CJIS-CT Security Policy with the goal to assure the confidentiality, integrity, and availability of CJI and Non CJI to the user community.
- Document and provide assistance for implementing the CJIS-CT security-related controls for the CJA.
- Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CJIS-CT Governing Board, State CSO, the affected criminal justice agency, and CSA ISO major incidents that significantly endanger the security or integrity of CJI and Non CJI.

3.1.7 CISS Administrator

The CISS administrator is employed by the State to perform the administration of CISS. The CISS administrator will have the ability to perform many functions, including the following:

- Administer agencies, roles, groups, groups of agencies, users and passwords system- wide.
- Save queries and reports to the Public Query Library.
- Administer all aspects of the CISS State Database containing State Data including managing indexes, backup/restore, configuration of system files, etc.
- Respond to automated system alerts or other problems and take corrective action as necessary.

3.1.8 Local Agency Security Officer (LASO)

Each Local Agency Security Officer (LASO) shall:

- Identify who is using the CJIS-CT Governing Board approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
- Identify and document how the equipment is connected to the CJIS-CT system.
- Ensure that personnel security screening procedures are being followed as stated in this Policy.
- Ensure the approved and appropriate security measures are in place and working as expected.
- Support policy compliance and ensure the CJIS-CT Governing Board ISO is promptly informed of security incidents.

3.1.9 CISS Community Agency Administrator (CAA)

The CISS Community Agency Administrator is employed by a specific agency to perform the administration of CISS. In general, the CISS Community Agency Administrator will have the ability to perform functions for users in their agency only. However, they may be designated by other agencies to perform their duties as well (Example: Department of Correction (DOC) and Board of Pardons and Parole (BOPP).
The functions they will be able to perform include the following:

- Administer agencies, roles, groups of agencies, users and expired passwords
- Save queries and reports to the Public Query Library

4. State Data, CJI Data, CHRI and Personally Identifiable Information

4.1 State Data

State data refers to all information housed, maintained, or processed by CJIS-CT that is provided by local, Tribal, State law enforcement and civil agencies. This data supports public safety, criminal justice, and civil operations and includes records used to fulfill each agency's respective statutory mission. State data encompasses, but is not limited to, criminal history, arrest records, case files, warrants, protective orders, motor vehicle information, and civil enforcement data.

4.2 Criminal Justice Information (CJI)

Criminal Justice Information is the 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. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

- Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include fingerprints, palm prints, iris scans, and facial recognition data.
- Identity History Data—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
- Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
- Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
- Case/Incident History—information about the history of criminal incidents.

The following types of data are exempt from the 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.

The intent of the CJIS-CT Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g., within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules. CJI introduced into the court system pursuant to a judicial proceeding that can be released to the public via a public records request is not subject to the CJIS-CT Security Policy.

4.3 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as "restricted data", is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI in accordance with CGS 54-142i. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.4 State Data and CJI Data Sources

The data sources for CISS include the following:

- OBIS : Offender Based Information System (OBIS) - Primary inmate management database of the Department of Correction (DOC). Tracks every individual from first intake through release
- PRAWN : Paperless Arrest Warrant Network (PRAWN) – Judicial system implemented in authorizing the court to enter warrants for criminal defendants who fail to appear for court in a central computer system. The PRAWN system was implemented in all municipal police departments in August 2005 and all state police units in March 2007.
- CRIM : Criminal / Motor Vehicle System (CRIM)) - The Superior Court's integrated case management application for criminal and motor vehicle dockets.
- MNI/CCH : Master Name Index & Computerized Criminal History (MNI/CCH) - DESPP State Police Bureau of Identification's fingerprint supported criminal history repository. Master Name Index links every identifier for a subject; CCH holds the arrest to disposition record required by CGS § 29 11. Supplies Connecticut's III rap sheet responses via COLLECT and NGI.
- COLLECT – WANTED : Within the Connecticut Online Law Enforcement Communications Teleprocessing System, the in state Wanted Person file (Collect – Wanted) stores active felony and misdemeanor warrants and mirrors NCIC's Wanted Person File for Connecticut inquiries as per CGS §§ 29 1 and 29 11.
- CMIS : Case Management Information System (CMIS) - Web based probation and pretrial supervision system run by the Judicial Branch Court Support Services Division. Holds adult & juvenile probation case data, risk assessments, program information, exchanges events.
- Case Notes : DOC community supervision tracking module (Case Notes) – These are separate from OBIS and used by Parole and Community Services officers to record field contacts, violations, and case plans.
- POR : Protection Order Registry (POR) - Judicial Branch automated registry of civil restraining orders, criminal protective orders, standing criminal restraining orders, and foreign orders filed in Connecticut regulated per CGS § 51 5c.
- SOR : Sex Offender Registry (SOR) - DESPP maintained registry of persons required to register under CGS §§ 54 251 to 54 254 (Chapter 969). Public facing site and law enforcement web service.
- CIB : Centralized Infractions Bureau (CIB) - Superior Court unit created per CGS § 51 164n that processes mail in traffic/boating infractions and minor violations.
- DMV : Department of Motor Vehicles Driver & Vehicle Records (DMV Files) - Master

files of driver licensing, vehicle registration, title, and insurance data maintained under CGS § 14 10. COLLECT provides read only CISS.

4.5 Access, Use and Dissemination of State, CJI and CHRI Data

4.5.1 Proper Access, Use, and Dissemination of State, CJI and CHRI Information

CHRI Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination of State, CJI and CHRI Data to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.5.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

In the event in the future CISS can accesses NCIC data with stakeholder approval the following requirements shall apply (CISS does not currently receive, store and disseminate FBI data).
The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

- Gang Files
- Threat Screening Center Files
- Supervised Release Files
- National Sex Offender Registry Files
- Historical Protection Order Files of the NCIC
- Identity Theft Files
- Protective Interest Files
- Person With Information (PWI) data in the Missing Person Files
- Violent Person File
- NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files

4.5.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

In the event in the future CISS can accesses NCIC data with stakeholder approval the following requirements shall apply (CISS does not currently receive, store and disseminate FBI data).

Whenever a Connecticut criminal justice agency queries or receives NCIC data through CISS, the rules govern how that information may be accessed, used, and disseminated

4.5.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.5.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with the inquiring agency's responsibility. Information obtained may be disseminated to
(a) other government agencies or
(b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.5.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.
A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

CSO Authority in Other Circumstances
If no federal, state or local law or policy prohibition exists, the State CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.6 Storage

When CISS State and CJI Data is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files.

4.7 Use of State Data and CJI for Research

Using State Data and Criminal Justice Information (CJI) for research purposes requires strict adherence to the CJIS-CT Security Policy and FBI's CJIS Security Policy (CSP) and relevant federal regulations. The goal is to protect State Data and Criminal Justice Information (CJI) while enabling valuable insights through responsible research.

4.7.1 Authorization & Legal Agreements

Formal approval must be obtained from the originating Criminal Justice Agency (CJA) or Noncriminal Justice Agency (NCJA) and CJIS-CT.
A written agreement must define the scope, purpose, use and data protection obligations.

All individuals with access to CJI must be approved, vetted and authorized by CJIS-CT.
CJIS-CT Security Addendum should be signed by agency requesting access State Data and CJI for research.

4.7.2 Permissible Use

State and CJI Data may be used for:

- Statistical analysis
- Historical or sociological research
- Scientific or policy studies

State and CJI Data must not be used for:

- Identify individuals (unless with explicit, legal consent)
- Interfere with ongoing criminal investigations
- Be used for commercial or non-authorized purposes

4.7.3 Data Protection Measures

To comply with the CJIS Security Policy, robust data protection controls must be in place:

i. Data Anonymization
   - Remove or transform personally identifiable information (PII) and case-specific identifiers.
   - Use techniques such as Suppression, Generalization (e.g., replacing exact ages with age ranges) and Aggregation (e.g., group-level statistics)

ii. Data Masking
   - Mask sensitive fields before sharing with researchers.
   - Use Static data masking (for datasets)
   - Use Dynamic masking (for controlled environments)

iii. Data Randomization

   Data randomization involves modifying the original data using statistical noise or perturbation, such that individual-level data is no longer accurate but aggregated insights remain valid.

   - Noise addition - Adds random values to data
   - Data swapping - Exchanges values between records
   - Micro-aggregation - Groups data and replaces values with the group average

iv. Encryption
   - Encrypt CJI at rest and in transit using FIPS 140-2 compliant algorithms.
   - Ensure keys are securely managed with strict access policies.

v. Access Controls
- Role-based access enforcement
- Strong multi-factor authentication (MFA)
- Session timeout and user activity logging

vi. Environmental Security
- Isolate research environments with Firewalls and intrusion detection
- Regular vulnerability scanning and patch management
- Physical access controls if research is conducted on-site

vii. Auditing & Logging
- Maintain complete logs of access and data handling.
- Logs must be Immutable and reviewed regularly
- Logs to be retained as per retention policy or minimum 1 year.

viii. Data Minimization
- Provide researchers with only the minimum data set necessary to achieve their objectives.
- Use synthetic data where feasible for early testing or modeling.

ix. Secure Disposal
- Ensure secure destruction or multi-pass overwrite sanitization of data and media post-research.

4.7.4 Oversight and Compliance

Research projects shall be subject to CJIS-CT security policy and FBI Security Policy compliance audits, data privacy reviews and third party audits.

4.7.5 Prohibited Uses

CJI must not be used for:

- Personal, political, or commercial gain
- Public exposure or dissemination without proper anonymization
- Cross-border sharing without proper legal basis
- Any usage violating 28 CFR Part 20, CJIS-CT Security Policy, FBI CJIS Security Policy or state laws

4.8 Justification and Penalties

4.8.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all State Data and CJI inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.8.2 Penalties

Improper access, use or dissemination of State and CJI is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.9 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an 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 as date and place of birth, or mother's maiden name. Any State and CJI Data provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

4.10 Commercial Distribution of State Data

Under no circumstance may State Data and CJI Data be distributed for commercial purposes.

5. Policy and Implementation

The policy areas focus upon the data and services that the CJIS-CT exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

Regardless of its form, use, or method of dissemination, CISS State and CJI Data requires protection throughout its life.

Not every consumer of CISS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

5.1-Information Exchange Agreements

5.2-Access Control

5.3-Awareness and Training

5.4-Audit and Accountability

5.5-Assessment, Authorization, and Monitoring

5.6-Configuration Management

5.7-Contingency Planning

5.8-Identification and Authentication

5.9-Incident Response

5.10-Maintenance

5.11-Media Protection

5.12-Physical and Environmental Protection

5.13-Planning

5.14-Personnel Security

5.15-Risk Assessment

5.16-Systems and Service Acquisition

5.17-System and Communications Protection

5.18-System and Information Integrity

5.19-Supply chain risk management

5.20-Mobile Devices

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Information exchanges shall be supported by documentation committing all parties to the terms of information exchange.

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.
Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.
Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs.
There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances, the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI.

Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing,
storing, and communication of State Data. These procedures apply to the exchange of State Data and CJI Data no matter the form of exchange.

The policies for information handling and protection also apply to using State Data and CJI Data shared with or received from CISS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations. Immigration and naturalization matters, and national security clearances.

5.1.1.1 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA or SIB

Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

5.1.1.2 Criminal Justice Agency User Agreement

Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere.
These agreements shall include:

i. Audit.
ii. Dissemination.
iii. Hit confirmation.
iv. Logging.
v. Quality Assurance (QA).
vi. Screening (Pre-Employment).
vii. Security.
viii. Timeliness.
ix. Training.
x. Use of the system.
xi. Validation.

5.1.1.3 Interagency and Management Control Agreements

An NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.4 Private Contractor User Agreements and CJIS-CT Security Addendum

The CJIS-CT Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS-CT Security Policy and the FBI CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.
Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the FBI CJISSecurity Addendum Certification page, and abide by all aspects of the FBI CJIS Security Addendum.

i. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to State Data and CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the FBI CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

ii. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.5 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to State data and CJI data. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to State data and CJI Data. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the FBI CJIS Security Policy. Each NCJA that directly accesses State Data and FBI CJI Data shall also allow CJIS-CT and FBI to periodically test the ability to penetrate the CJIS-CT and FBI's network through the external network connection or system.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, CJIS-CT, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.3 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by CJIS-CT, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.4 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log on such dissemination.

5.1.5 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement, then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

5.2 Policy Area 2: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS-CT information and the modification of information systems, applications, services and communication configurations allowing access to CJIS-CT information.

5.2.1 Account Management

CJIS-CT shall manage information system accounts or profiles, including establishing, activating, modifying, reviewing, disabling, and removing accounts or profiles. CJIS-CT shall validate information system accounts or profiles at least annually and shall document the validation process. The validation and documentation of accounts or profiles can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. CJIS-CT shall identify authorized users of the information system and specify access rights/privileges. CJIS-CT shall grant access to the information system based on:

i. Valid need-to-know/need-to-share that is determined by assigned official duties.
ii. Satisfaction of all personnel security criteria.
iii. When CJIS-CT is responsible for account management it shall be notified when:
iv. A user's information system usage or need-to-know or need-to-share changes.
v. A user is terminated or transferred or associated accounts or profiles are removed, disabled, or otherwise secured.
vi. All privileged accounts accessing State Data must use multi-factor authentication (MFA). Authentication methods must meet NIST 800-63B standards and be reviewed annually for compliance.

5.2.2 Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

5.2.2.1 Least Privilege

The agency shall approves individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know. Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

5.2.2.2 System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems:

i. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
ii. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

5.2.2.3 Access Control Criteria

CJIS-CT shall control access to State and CJI data based on one or more of the following:

i. Job assignment or function (i.e., the claims) of the user seeking access.
ii. Physical location.
iii. Logical location.
iv. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
v. Time-of-day and day-of-week/month restrictions.

5.2.2.4 Access Control Mechanisms

When setting up access controls, CJIS-CT shall use one or more of the following mechanisms:

i. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
ii. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.
iii. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is

Federal Information Processing Standards (FIPS) 140-2 (as amended) compliant.

iv. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

5.2.3 Unsuccessful Login Attempts to the CISS Portal

Where technically feasible, the system shall enforces a limit of no more than five (5) consecutive invalid access attempts by a user (attempting to access State Data and CJI Data or systems with access to State Data). The system shall automatically lock the account/node for a ten (10) minute time period unless released by an administrator.

5.2.4 System Use Notification

The information system shall display an approved system use notification message before granting access, informing potential users of various usages and monitoring rules. The system notification message shall, at a minimum, provide the following information:

i. The user is accessing a restricted information system.
ii. System usage may be monitored, recorded, and subject to audit.
iii. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
iv. Use of the system indicates consent to monitoring and recording.

The system notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system.

For publicly accessible systems:

- The system use information is available and, when appropriate, is displayed before granting access
- Any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities
- The notice given to public users of the information system includes a description of the authorized uses of the system

5.2.5 Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are:

i. part of a criminal justice conveyance.
ii. used to perform dispatch functions and located within a physically secure location.
iii. terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.

Note: an example of a session lock is a screen saver with password.

5.2.6 Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).
The agency shall employs automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.
Virtual escorting of privileged functions is permitted only when all the following conditions are met:

i. The session shall be monitored at all times by an authorized escort
ii. The escort shall be familiar with the system/area in which the work is being performed.
iii. The escort shall have the ability to end the session at any time.
iv. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
v. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

5.2.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CISS State and CJI Data unless the CJIS-CT has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e., bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area: Mobile Devices.
This control does not apply to the use of personally owned information systems to access agency's

information systems and information that are intended for public access. (e.g., an agency's public Website that contains purely public information).

5.2.6.2 Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit State Data. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

5.3 Policy Area 3: Awareness and Training

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

5.3.1 Security Training and Awareness

i. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
   a. As part of initial training for new users prior to accessing CJI and annually thereafter.
   b. When required by system changes or within 30 days of any security event for individuals involved in the event.

ii. Employ one or more of the following techniques to increase the security and privacy awareness of system users:
   a. Displaying posters
   b. Offering supplies inscribed with security and privacy reminders
   c. Displaying logon screen messages
   d. Generating email advisories or notices from organizational officials
   e. Conducting awareness events

iii. Update literacy training and awareness content annually and following changes in the information system operating environment, when security incidents occur, or when changes are made in the CJIS-CT Security Policy.

iv. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

v. Provide literacy training on recognizing and reporting potential indicators of insider threat.

vi. Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

5.3.2 Role Based Training

5.3.2.1 Provide role-based security and privacy training to personnel with the following roles and responsibilities:

i. All individuals with unescorted access to a physically secure location.

ii. General User: A user, but not a process, who is authorized to use an information system.

iii. Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform.

iv. 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-CT Security policy.

   a. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter.
   b. When required by system changes.

5.3.2.2 Update role-based training content annually and following audits of the CSA and local agencies; changes in the information system operating environment; security incidents; or when changes are made to the CJIS-CT Security Policy.

5.3.2.3 Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

5.3.2.4 Incorporate the minimum following topics into the appropriate role-based training content:

i. All individuals with unescorted access to a physically secure location
   a. Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties
   b. Reporting Security Events
   c. Incident Response Training
   d. System Use Notification
   e. Physical Access Authorizations
   f. Physical Access Control
   g. Monitoring Physical Access
   h. Visitor Control
   i. Personnel Sanctions

ii. General User: A user, but not a process, who is authorized to use an information system.
   a. Criminal Justice Information
   b. Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information
   c. Personally Identifiable Information
   d. Information Handling
   e. Media Storage
   f. Media Access
   g. Audit Monitoring, Analysis, and Reporting
   h. Access Enforcement
   i. Least Privilege
   j. System Access Control
   k. Access Control Criteria
   l. System Use Notification
   m. Session Lock
   n. Personally Owned Information Systems
   o. Password
   p. Access Control for Display Medium
   q. Encryption
   r. Malicious Code Protection
   s. Spam and Spyware Protection
   t. Cellular Devices
   u. Mobile Device Management
   v. Wireless Device Risk Mitigations
   w. Wireless Device Malicious Code Protection
   x. Literacy Training and Awareness/Social Engineering and Mining
   y. Identification and Authentication (Organizational Users)
   z. Media Protection

iii. Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform.
   a. Access Control
   b. System and Communications Protection and Information Integrity
   c. Patch Management
   d. Data backup and storage—centralized or decentralized approach
   e. Most recent changes to the CJIS-CT Security Policy

iv. 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-CT Security Policy.

   a. Local Agency Security Officer Role
   b. Authorized Recipient Security Officer Role
   c. Additional state/local/tribal/territorial or federal agency roles and responsibilities
   d. Summary of audit findings from previous state audits of local agencies
   e. Findings from the last FBI CJIS Division audit

5.3.2.5 Role-Based Training | Processing Personally Identifiable Information

i. Provide all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls.

5.3.3 Training Records

i. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training.
ii. Retain individual training records for a minimum of three years.

5.4 Policy Area 4: Audit and Accountability

CJIS-CT shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. CJIS-CT shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within CJIS-CT. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with CJIS-CT's assessment of risk.

i. Develop procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls.
ii. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the audit and accountability procedures.
iii. Review and Update procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
iv. CJIS-CT shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week.

5.4.1 Event Logging

i. Identify the types of events that the system is capable of logging in support of the audit function: authentication, file use, user/group management, events sufficient to establish what occurred, the sources of events, outcomes of events, and operational transactions (e.g., NCIC, III).
ii. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged.
iii. Specify the following event types for logging within the system:
   All successful and unsuccessful:
   a. System log-on attempts
   b. Attempts to use:
      - Access permission on a user account, file, directory, or other system resource.
      - Create permission on a user account, file, directory, or other system resource.
      - Write permission on a user account, file, directory, or other system resource.
      - Delete permission on a user account, file, directory, or other system resource.
iv. Change permission on a user account, file, directory, or other system resource.
   a. Attempts to change account passwords
   b. Actions by privileged accounts
   c. Attempts for users to:

- Access the audit log file.
- Modify the audit log file.
- Destroy the audit log file.
- Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents.
- Review and update the event types selected for logging annually.

v. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents.
vi. Review and update the event types selected for logging annually.

5.4.2 Content of audit records including additional audit information.

Ensure that audit records contain information that establishes the following:

i. What type of event occurred.
ii. When the event occurred.
iii. Where the event occurred.
iv. Source of the event.
v. Outcome of the event.
vi. Identity of any individuals, subjects, or objects/entities associated with the event.
vii. Session, connection, transaction, and activity duration.
viii. Source and destination addresses.
ix. Object or filename involved.
x. Number of bytes received, and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.
xi. The III portion of the log shall clearly identify:
    a. The operator
    b. The authorized receiving agency
    c. The requestor
    d. The secondary recipient
xii. Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: minimum PII necessary to achieve the purpose for which it is collected.

5.4.3 Audit Log Storage

i. Allocate audit log storage capacity to accommodate the collection of audit logs to meet retention requirements.

5.4.4 Response to Audit Logging Process Failures

i. Alert organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure.
ii. Take the following additional actions: restart all audit logging processes and verify system(s) are logging properly.
iii. Inform the State CSO and CJIS-CT ISO on the security incidents due to the logging process failures

5.4.5 Audit Record Review, Analysis, and Reporting

i. Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity.
ii. Report findings to organizational personnel with audit review, analysis, and reporting responsibilities and organizational personnel with information security and privacy responsibilities.
iii. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.
iv. Integrate audit record review, analysis, and reporting processes using automated mechanisms.
v. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

5.4.6 Audit Record Reduction and Report Generation

Provide and implement an audit record reduction and report generation capability that:

i. Supports on-demand audit record review, analysis, and reporting requirements and after- the-fact investigations of incidents.
ii. Does not alter the original content or time ordering of audit records.
iii. Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content

5.4.7 Time Stamps

i. Use internal system clocks to generate time stamps for audit records.
ii. Record time stamps for audit records that meet hundredths of a second (i.e., hh:mm:ss:00) interval and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

5.4.8 Protection of Audit Information

i. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
ii. Alert organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators upon detection of unauthorized access, modification, or deletion of audit information.
iii. Authorize access to management of audit logging functionality to only organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators.

5.4.9 Audit Record Retention

i. Retain audit records for a minimum of one (1) year or until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention.

5.4.10 Audit Record Generation

i. Provide audit record generation capability for the event types the system is capable of auditing as defined above on all systems generating required audit logs.
ii. Allow organizational personnel with audit record generation responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators to select the event types that are to be logged by specific components of the system.
iii. Generate audit records for the event types defined above that include all the defined audit record content.

5.5 Policy Area 5: Assessment, Authorization, and Monitoring

5.5.1 Procedures

i. Develop procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls.
ii. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring procedures.
iii. Review and update the Procedures annually and following changes to the assessment criteria.

5.5.2 Control Assessments

i. Select the appropriate assessor or assessment team for the type of assessment to be conducted.
ii. Develop a control assessment plan that describes the scope of the assessment including:
iii. Controls and control enhancements under assessment.
   a. Assessment procedures to be used to determine control effectiveness.
   b. Assessment environment, assessment team, and assessment roles and responsibilities.
   c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment.
iv. Assess the controls in the system and its environment of operation and any controls that have been impacted by evolving threats at least once every three years to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements.
v. Produce a control assessment report that documents the results of the assessment.
vi. Provide the results of the control assessment report to the individual who executed the CJIS-CT User Agreement or is in contact with the CJIS-CT.
vii. Employ independent assessors or assessment teams to conduct control assessments.

5.5.3 Information Exchange

Approve and manage the exchange of information between the agency system and external systems using the following agreements when applicable.

i. Executed CJIS-CT User Agreements

   a. Each CSA, SIB, or IA shall execute a signed written agreement with CJIS-CT stating their willingness to demonstrate conformity with the CJIS-CT Security Policy and FBI CJIS Security Policy before accessing and consuming State Data and CJI as set forth in the agreement.
   b. The agreement shall include the standards, audit, and sanctions governing utilization of CJIS-CT.
   c. CJIS-CT is authorized to periodically test the ability to penetrate the CJIS-CT Network

through the external connection or system upon proper notification of all signatories in the user agreement.

ii. Criminal Justice Agency User Agreements

Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access.
The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

a. Audit
b. Dissemination
c. Hit confirmation
d. Logging
e. Quality Assurance (QA)
f. Screening (Criminal Justice Employment)
g. Security
h. Timeliness
i. Training
j. Use of the system
k. Validation

iii. Agreements for Noncriminal Justice Use of CHRI

A CJA, NCJA (public), or NCJA (private) designated to request civil fingerprint-based background checks, with full consent of the individual to whom the background check is taking place, for noncriminal justice functions, shall be eligible for access to CHRI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. The CJA, NCJA (public), or NCJA (private) receiving access to CHRI shall enter into signed written agreements with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. The written agreement shall specify the policies to which the agency must adhere, which include all pertinent areas of the CJISSECPOL. Each NCJA that directly accesses FBI systems shall allow the FBI to periodically test the ability to penetrate the FBI's network through the external connection or system. A CJA, NCJA (public), or NCJA (private) authorized to access CHRI for noncriminal justice functions pursuant to federal law or state statute approved by the U.S. Attorney General (defined by the Compact Council as an Authorized Recipient), cannot make CHRI available to another governmental agency, nongovernmental agency, or private contractor to perform noncriminal justice administrative functions without implementation of one of the following:

a. Security and Management Control Outsourcing Standard for Non-Channelers. Implementation is applicable to noncriminal justice administrative functions that do not require a direct connection to the FBI for submission of fingerprints and receipt of CHRI. Examples include making fitness determinations, processing, storing, or destroying documents, and maintaining IT platforms that do not connect to CJIS-CT systems. Prior to implementation, Authorized Recipients must request and receive written permission from the State Compact Officer, Chief Administrator of the state's criminal history record repository, or the FBI Compact Officer, as applicable.

b. Security and Management Control Outsourcing Standard for Channeling. Implementation is applicable only to Channeling functions performed by an FBI-approved Channeler that require a direct connection to the FBI for submission of fingerprints and receipt of CHRI. Prior to implementation, Authorized Recipients must request and receive written permission from the State Compact Officer, Chief Administrator of the state's criminal history record repository, or the FBI Compact Officer, as applicable.

c. Management Control Agreement or Security Addendum (see Appendix H) pursuant to Title 28, C.F.R., Section 20.33 (a) (6) or (7). Although by regulation implementation of a Management Control Agreement or the Security Addendum is applicable to the administration of criminal justice pursuant to that agreement performed on behalf of CJAs, under very limited circumstances, implementation may also be applicable to CJAs that obtain and use CHRI for noncriminal justice purposes. Implementation for noncriminal justice purposes is only applicable when another governmental agency or private contractor performs both criminal justice and noncriminal justice administrative functions involving access to CHRI on behalf of the CJA. It is important to note that if the servicing governmental agency or private contractor solely performs noncriminal justice administrative functions, then the CJA would be required to implement the Security and Management Control Outsourcing Standard for Non-Channelers.

iv. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated.

v. Review and update the agreements at least triennially or when responsibilities or signatories change.

vi. Secondary Dissemination

a. Log the dissemination of CHRI when released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s). If CJI does not contain CHRI and is not part of an information exchange agreement, then it does not need to be logged.

b. Validate the requestor of CJI in conformance with the local policy as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission; or a member of the public receiving CJI via authorized dissemination.

5.5.4 Plan of Action and Milestones

i. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system.
ii. Update existing plan of action and milestones at least every six (6) months or when new information is available based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

5.5.5 Authorization

i. Assign a senior official as the official responsible for the system.
ii. Assign the CSO, SIB Chief, or IA Official as the authorizing official for common controls available for inheritance by organizational systems.
iii. Ensure that the official authorizes the system before commencing operations:
    a. Accepts the use of common controls inherited by the system.
    b. Authorizes the system to operate.
iv. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems.
v. Update the authorizations at least every three (3) years.

5.5.6 Continuous Monitoring

i. Establishing the following system-level metrics to be monitored

    a. Account Management
    b. Remote Access | Monitoring and Control
    c. Training Records
    d. Configuration Change Control
    e. Configuration Settings
    f. User-Installed Software
    g. Incident Monitoring
    h. Controlled Maintenance
    i. Maintenance Tool
    j. Nonlocal Maintenance
    k. Physical Access Control
    l. Monitoring Physical Access
    m. Environmental Controls
    n. Delivery and Removal
    o. External Personnel Security
    p. External System Services
    q. Boundary Protection
    r. Boundary Protection | Personally Identifiable Information
    s. Mobile Code
    t. System Monitoring

ii. Establishing an ongoing frequency for monitoring and an ongoing frequency for assessment of control effectiveness.

iii. Ongoing control assessments in accordance with the continuous monitoring strategy.

iv. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy.

v. Correlation and analysis of information generated by control assessments and monitoring.

vi. Response actions to address results of the analysis of control assessment and monitoring information.

vii. Reporting the security and privacy status of the system to organizational personnel with information security, privacy responsibilities, and system/network administrators annually, when security events/incidents occur, and when requested.

5.6 Policy Area 6: Configuration Management

5.6.1 Configuration Management Policy includes,

i. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the configuration management policy and procedures.

ii. Review and update the current configuration management:
   a. Policy annually and following any hardware or software changes to systems which process, store, or transmit CJI.
   b. Procedures annually and following any hardware or software changes to systems which process, store, or transmit CJI.

5.6.2 Baseline Configuration

i. Develop, document, and maintain under configuration control, a current baseline configuration of the system.
ii. Develop, document, and maintain a current and complete topological drawing depicting the interconnectivity of the agency network to criminal justice information systems and services.
iii. Review and update the baseline configuration and topological drawing of the system.

   a. At least annually.
   b. When required due to security-relevant changes to the system and/or security incidents occur.
   c. When system components are installed or upgraded.

iv. Retain at least one (1) previous version of baseline configurations of the system to support rollback.

5.6.3 Configuration Change Control

i. Determine and document the types of changes to the system that are configuration controlled.
ii. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analysis.
iii. Document configuration change decisions associated with the system.
iv. Implement approved configuration-controlled changes to the system.
v. Retain records of configuration-controlled changes to the system for two (2) years.
vi. Monitor and review activities associated with configuration-controlled changes to the system.
vii. Coordinate and provide oversight for configuration change control activities through personnel with configuration management responsibilities, a Configuration Control Board, or Change Advisory Board that convenes regularly or when hardware or software changes (i.e., updates,

upgrades, replacements, etc.) to the information system are required.

viii. Establish document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using established best practices and guidelines such as Defense Information Systems Agency (DISA) Secure Technical Implementation Guidelines (STIGs), Center for Internet Security (CIS) Benchmarks, or Federal Information Processing Standards.

ix. Implement the configuration settings.

x. Identify, document, and approve any deviations from established configuration settings for system components that store, process, or transmit CJI based on operational requirements.

xi. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

5.6.4 Configuration Change Control – Testing, Validation and Documentation of changes

i. Test, validate, and document changes to the system before finalizing the implementation of the changes.

5.6.5 Configuration Change Control – Security and Privacy Representatives

i. Require organizational personnel with information security and privacy responsibilities to be members of the Configuration Control Board or Change Advisory Board.

5.6.6 Configuration Change Control – Impact Analysis

i. Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

ii. After-system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

iii. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

5.6.7 Least Functionality

i. Configure the system to provide only essential capabilities to meet operational requirements.

ii. Prohibit or restrict the use of specified functions, ports, protocols, software, and/or services which are not required.

iii. Review the system annually, as the system changes, or incidents occur to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services.

iv. Disable or remove functions, ports, protocols, software, and/or services within the system deemed to be unnecessary and/or unsecure.

v. Prevent program execution in accordance with rules of behavior and/or rules authorizing the
vi. Identify software programs authorized to execute on the system.
vii. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.
viii. Review and update the list of authorized software programs annually.

5.6.8 System Component Inventory

i. Develop and document an inventory of system components that:
   a. Accurately reflects the system.
   b. Includes all components within the system.
   c. Does not include duplicate accounting of components or components assigned to any other system.
   d. Is at the level of granularity deemed necessary for tracking and reporting.
   e. Includes the following minimum information to achieve system component accountability: date of installation, model, serial number, manufacturer, supplier information, component type, software owner, software version number, software license information, and hardware and physical location.

ii. Review and update the system component inventory annually.
iii. Update the inventory of system components as part of component installations, removals, and system updates.
iv. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms continuously or at least weekly.
v. Take the following actions when unauthorized components are detected: disable or isolate the unauthorized components and notify organizational personnel with security responsibilities.

5.6.9 Configuration Management Plan

Develop, document, and implement a configuration management plan for the system that:

i. Addresses roles, responsibilities, and configuration management processes and procedures.
ii. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.
iii. Defines the configuration items for the system and places the configuration items under configuration management.
iv. Is reviewed and approved by organizational personnel with information security responsibilities and organizational personnel with configuration management responsibilities.
v. Protects the configuration management plan from unauthorized disclosure and modification.

5.6.10 Software Usage Restrictions

i. Use software and associated documentation in accordance with contract agreements and copyright laws.
ii. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.
iii. Control and document the use of peer-to-peer file sharing technology to ensure that this capability

is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

iv. Establish agency-level policies governing the installation of software by users;

v. Enforce software installation policies through automated methods.

vi. Monitor policy compliance through automated methods at least weekly.

5.6.11 Information Location

i. Identify and document the location of CJI and the specific system components on which the information is processed, stored, or transmitted.

ii. Identify and document the users who have access to the system and system components where the information is processed and stored.

iii. Document changes to the location (i.e., system or system components) where the information is processed and stored.

iv. Use automated tools to identify CJI on software and hardware system components to ensure controls are in place to protect organizational information and individual privacy.

5.6.12 Network Diagram

CJIS-CT ISO shall ensure that a complete topological drawing depicting the interconnectivity of the CJIS-CT network, to agency/criminal justice information, systems and services is maintained in a current status and shall be on file with the CJIS-CT ISO.
The network topological drawing shall include the following:

i. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency endpoint.

ii. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not need to be shown; the number of clients is sufficient.

iii. For Official Use Only markings.

iv. The date (day, month, and year) the drawing was created or updated.

5.6.13 Security of Configuration Management

The system configuration documentation often contains sensitive details (e.g., descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) CJIS-CT ISO shall protect the system documentation from unauthorized access consistent with the provisions as described in Access Control.

5.7 Policy Area 7 – Contingency Planning (CP)

5.7.1 Contingency Plan and Identification of Critical Assets

i. Develop a contingency plan for the system that.

   a. Identifies essential mission and business functions and associated contingency requirements.
   b. Provides recovery objectives, restoration priorities, and metrics.
   c. Addresses contingency roles, responsibilities, assigned individuals with contact information.
   d. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure.
   e. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented.
   f. Addresses the sharing of contingency information.
   g. Is reviewed and approved by agency head or their designee.

ii. Distribute copies of the contingency plan to organizational personnel with contingency planning or incident response duties.
iii. Coordinate contingency planning activities with incident handling activities.
iv. Review the contingency plan for the system annually.
v. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
vi. Communicate contingency plan changes to organizational personnel with contingency planning or incident response duties.
   a. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training.
   b. Protect the contingency plan from unauthorized disclosure and modification.
   c. Coordinate contingency plan development with organizational elements responsible for related plans.
   d. Plan for the resumption of essential mission and business functions within twenty-four (24) hours of contingency plan activation.
   e. Identify critical system assets supporting essential mission and business functions.

5.7.2 Contingency Training

i. Provide contingency training to system users consistent with assigned roles and responsibilities:
   a. Within thirty (30) days of assuming a contingency role or responsibility.
   b. When required by system changes.
   c. Annually thereafter.

ii. Review and update contingency training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises.

5.7.3 Contingency Plan Testing

i. Test the contingency plan for the system annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), or comprehensive exercises. Plans related to contingency planning for organizational systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans

ii. Review the contingency plan test results.

iii. Initiate corrective actions, if needed.

iv. Coordinate contingency plan testing with organizational elements responsible for related plans

5.7.4 Alternate Storage Site

i. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information.

ii. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

iii. Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

iv. Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

v. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

5.7.4 Alternate Processing Site

i. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of operations for essential mission and business functions within the time period defined in the system contingency plan(s) when the primary processing capabilities are unavailable.

ii. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption.

iii. Provide controls at the alternate processing site that are equivalent to those at the primary site.

iv. Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

v. Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

vi. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

5.7.5 Telecommunications Services

i. Establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within the time period as defined in the system contingency plan(s) when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
ii. Develop primary and alternate telecommunications service agreements that contain priority of service provisions in accordance with availability requirements (including recovery time objectives).
iii. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.
iv. Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

5.7.6 Backup

i. Conduct backups of user-level information contained in operational systems for essential business functions as required by the contingency plans.
ii. Conduct backups of system-level information contained in the system as required by the contingency plans.
iii. Conduct backups of system documentation, including security- and privacy-related documentation as required by the contingency plans.
iv. Protect the confidentiality, integrity, and availability of backup information.
v. Test backup information as required by the contingency plans to verify media reliability and information integrity.
vi. Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of CJI.
vii. The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of the mechanisms selected is commensurate with the security category or classification of the information. Cryptographic protection applies to system backup information in storage at both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

5.7.7 System Recovery and Reconstitution

i. Provide for the recovery and reconstitution of the system to a known state within the timeframe as required by the contingency plans after a disruption, compromise, or failure.
ii. Recovery is executing contingency plan activities to restore organizational mission and business functions.
iii. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states.

iv. Recovery and reconstitution operations reflect mission and business priorities, recovery point, recovery time, and reconstitution objectives. organizational metrics consistent with contingency plan requirements.

v. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations.

vi. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures.

vii. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.

viii. Implement transaction recovery for systems that are transaction-based. Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.

5.8 Policy Area 8 – Identification and Authentication

CJIS-CT shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.
Each person who is authorized to store, process, and/or transmit State and CJI Data shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access State and CJI Data or networks leveraged for State and CJI Data transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

Use of originating agency identifiers in transactions and information exchanges

An authorized originating agency identifier (ORI) shall be used in each transaction on CJIS-CT systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CJIS-CT shall be the originating agency identifier (ORI), and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction
may not necessarily be the same as the agency requesting the transaction, CJIS-CT shall ensure that the ORI for each transaction can be traced, via the audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned to limited access ORI shall not use the full access ORI of another agency to conduct an inquiry transaction

5.8.1 Identification and Authentication

i. Develop, document, and disseminate to authorized personnel:
    a. Agency/Entity identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
    c. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls.

ii. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the identification and authentication policy and procedures.

iii. Review and update the current identification and authentication:
   a. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
   b. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

5.8.2 Identification and Authentication – Organizational Users

i. Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users
ii. Implement multi-factor authentication for access to privileged accounts.
iii. Implement multi-factor authentication for access to non-privileged accounts.
iv. Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts
v. Accept and electronically verify Personal Identity Verification-compliant credentials

5.8.3 Identification and Authentication – Devices

i. Uniquely identify and authenticate agency-managed devices before establishing network connections. In the instance of local connection, the device must be approved by the agency and the device must be identified and authenticated prior to connection to an agency asset.

5.8.4 Identification and Authentication – Identifier Management

Manage system identifiers by:

i. Receiving authorization from organizational personnel with identifier management responsibilities to assign an individual, group, role, service, or device identifier.
ii. Selecting an identifier that identifies an individual, group, role, service, or device.
iii. Assigning the identifier to the intended individual, group, role, service, or device.
iv. Preventing reuse of identifiers for one (1) year.
v. Manage individual identifiers by uniquely identifying each individual as agency or nonagency.

5.8.5 Authenticator Management

Manage system authenticators by:

i. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator.
ii. Establishing initial authenticator content for any authenticators issued by the organization.
iii. Ensuring that authenticators have sufficient strength of mechanism for their intended use.
iv. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators.
v. Changing default authenticators prior to first use.
vi. Changing or refreshing memorized secret authenticators annually or when there is evidence of

authenticator compromise; changing or refreshing all other authenticator types as they expire or when there is evidence of authenticator compromise.

vii. Protecting authenticator content from unauthorized disclosure and modification.

viii. Requiring individuals to take, and having devices implement, specific controls to protect authenticators.

ix. Changing authenticators for group or role accounts when membership to those accounts changes.

x. AAL2 Specific Requirements: All credential service providers (CSPs) authenticating claimants at Authenticator Assurance Level 2 (AAL2) SHALL be assessed on the following criteria:
   a. Authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators.
   b. If the multi-factor authentication process uses a combination of two single-factor authenticators, then it SHALL include a Memorized Secret authenticator and a possession-based authenticator.
   c. Cryptographic authenticators used at AAL2 SHALL use approved cryptography.
   d. At least one authenticator used at AAL2 SHALL be replay resistant.
   e. Communication between the claimant and verifier SHALL be via an authenticated protected channel.
   f. Verifiers operated by government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1.
   g. Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1.
   h. If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors.
   i. If a biometric factor is used in authentication at AAL2, then the performance requirements stated in Biometric Requirements SHALL be met.
   j. Reauthentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session.
   k. Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer.
   l. The CSP SHALL comply with records retention policies in accordance with applicable laws and regulations.

xi. If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and SHALL inform subscribers of that retention policy.

xii. Privacy requirements that apply to all credential service providers (CSPs), verifiers, and Relying Parties (RPs).

   a. The CSP SHALL employ appropriately tailored privacy controls from the CJIS-CT Security Policy.
   b. If the CSP processes attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively “identity service”), related fraud mitigation, or to comply with law or legal process, then the CSP SHALL implement measures to maintain predictability and manageability commensurate with the associated privacy risk.

xiii. General requirements applicable to AAL2 authentication process.

a. CSPs SHALL provide subscriber instructions on how to appropriately protect a physical authenticator against theft or loss.
b. The CSP SHALL provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.
c. If required by the authenticator type descriptions in IA-5(1), then the verifier SHALL implement controls to protect against online guessing attacks.
d. If required by the authenticator type descriptions in IA-5(1) and the description of a given authenticator does not specify otherwise, then the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100.

Supplemental Guidance :

Throttling or rate limiting is key to resistance against online guessing attacks. It is important that it be implemented in a non-abrupt manner as described in the specification so that it is not usable as a denial-of-service mechanism by an attacker. Additional techniques MAY be used to reduce the likelihood that an attacker will lock the legitimate claimant out as a result of rate limiting. These include:

- Requiring the claimant to complete a CAPTCHA before attempting authentication.
- Requiring the claimant to wait following a failed attempt for a period of time that increases as the account approaches its maximum allowance for consecutive failed attempts (e.g., 30 seconds up to an hour).
- Accepting only authentication requests that come from a whitelist of IP addresses from which the subscriber has been successfully authenticated before. Leveraging other risk-based or adaptive authentication techniques to identify user behavior that falls within, or out of, typical norms. These might, for example, include use of IP address, geolocation, timing of request patterns, or browser metadata.

e. If signed attestations are used, then they SHALL be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of 112 bits as of the date of this publication.
f. If the verifier and CSP are separate entities, then communications between the verifier and CSP SHALL occur through a mutually authenticated secure channel (such as a client-authenticated TLS connection).
g. If the CSP provides the subscriber with a means to report loss, theft, or damage to an authenticator using a backup or alternate authenticator, then that authenticator SHALL be either a memorized secret or a physical authenticator.
h. If the CSP chooses to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised, then...The suspension SHALL be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.
i. If and when an authenticator expires, it SHALL NOT be usable for authentication.
j. The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator.

k. CSPs SHALL revoke the binding of authenticators immediately upon notification when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.
l. The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing certified attributes signed by the CSP within five (5) days after revocation or termination takes place.

xiv. Biometric Requirements

a. Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (something you have).
b. An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established.
c. The sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant.
d. The biometric system SHALL operate with an False Match Rate (FMR) of 1 in 1000 or better. This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt).
e. The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD demonstrating at least 90% resistance to presentation attacks is implemented.

xv. Once the limit on authentication failures has been reached, the biometric authenticator SHALL either:

a. Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt, or
b. disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available.
c. The verifier SHALL make a determination of sensor and endpoint performance, integrity, and authenticity.
d. If biometric comparison is performed centrally, then use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are identified using approved cryptography.
e. If biometric comparison is performed centrally, then a separate key SHALL be used for identifying the device.
f. If biometric comparison is performed centrally, then biometric revocation, referred to as biometric template protection SHALL be implemented.
g. If biometric comparison is performed centrally, all transmission of biometrics SHALL be over the authenticated protected channel.
h. Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing SHALL be zeroized immediately after any training or research data has been derived.

xvi. Authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used — possibly in conjunction with other authenticators — to authenticate for that account.

a. Authenticators SHALL be bound to subscriber accounts by either issuance by the CSP as part of enrollment or associating a subscriber-provided authenticator that is acceptable to the CSP.
b. Throughout the digital identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with each identity.
c. The CSP or verifier SHALL maintain the information required for throttling authentication attempts.
d. The CSP SHALL also verify the type of user-provided authenticator so verifiers can determine compliance with requirements at each AAL.
e. The record created by the CSP SHALL contain the date and time the authenticator was bound to the account.
f. When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at AAL2.
g. Protocols for key provisioning SHALL use authenticated protected channels or be performed in person to protect against MitM attacks.
h. Binding multi-factor authenticators SHALL require multi-factor authentication (or equivalent) at identity proofing.
i. At enrollment, the CSP SHALL bind at least one, and SHOULD bind at least two, physical (something you have) authenticators to the subscriber's online identity, in addition to a memorized secret or one or more biometrics.
j. At enrollment, authenticators at AAL2 and IAL2 SHALL be bound to the account.
k. If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then the applicant SHALL identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant's phone number, email address, or postal address of record.
l. If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then long-term authenticator secrets are delivered to the applicant within a protected session.
m. If enrollment and binding are being done in person and cannot be completed in a single physical encounter, the applicant SHALL identify themselves in person by either using a secret or through use of a biometric that was recorded during a prior encounter.
n. If enrollment and binding are being done in person and cannot be completed in a single physical encounter, temporary secrets SHALL NOT be reused.
o. If enrollment and binding are being done in person and cannot be completed in a single physical encounter and the CSP issues long-term authenticator secrets during a physical transaction, they SHALL be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.
p. Before adding a new authenticator to a subscriber's account, the CSP SHALL first require the subscriber to authenticate at AAL2 (or a higher AAL) at which the new authenticator will be used.
q. If the subscriber's account has only one authentication factor bound to it, the CSP SHALL require the subscriber to authenticate at
r. If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2, that subscriber SHALL repeat the identity proofing process.
s. If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2 or IAL3, the CSP SHALL require the claimant to authenticate using an authenticator of the remaining factor, if any, to confirm binding to the existing identity.
t. If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then it requires entry of a confirmation code sent to an address of record.
u. If the CSP opts to allow binding of a new memorized secret with the use of two physical

authenticators, then the confirmation code SHALL consist of at least 6 random alphanumeric characters generated by an approved random bit generator.

v. If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL be valid for a maximum of 7 days but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service. Confirmation codes sent by means other than physical mail SHALL be valid for a maximum of 5 minutes.

xvii. Session Management: The following requirements apply to applications where a session is maintained between the subscriber and relying party to allow multiple interactions without repeating the authentication event each time. Once an authentication event has taken place, it is often desirable to allow the subscriber to continue using the application across multiple subsequent interactions without requiring them to repeat the authentication event. This requirement is particularly true for federation scenarios where the authentication event necessarily involves several components and parties coordinating across a network.

a. Session Binding Requirements: A session occurs between the software that a subscriber is running — such as a browser, application, or operating system (i.e., the session subject) and the RP or CSP that the subscriber is accessing (i.e., the session host).
b. A session is maintained by a session secret which SHALL be shared between the subscriber's software and the service being accessed.
c. The secret SHALL be presented directly by the subscriber's software or possession of the secret SHALL be proven using a cryptographic mechanism.
d. The secret used for session binding SHALL be generated by the session host in direct response to an authentication event.
e. A session SHALL NOT be considered at a higher AAL than the authentication event.
f. Secrets used for session binding SHALL be generated by the session host during an interaction, typically immediately following authentication.
g. Secrets used for session binding SHALL be generated by an approved random bit generator.
h. Secrets used for session binding SHALL contain at least 64 bits of entropy.
i. Secrets used for session binding SHALL be erased or invalidated by the session subject when the subscriber logs out.
j. Secrets used for session binding SHALL be sent to and received from the device using an authenticated protected channel.
k. Secrets used for session binding SHALL time out and not accepted after the specified times.
l. Secrets used for session binding SHALL NOT be available to insecure communications between the host and subscriber's endpoint.
m. Authenticated sessions SHALL NOT fall back to an insecure transport, such as from https to http, following authentication.
n. URLs or POST content SHALL contain a session identifier that SHALL be verified by the RP to ensure that actions taken outside the session do not affect the protected session.
o. Browser cookies SHALL be tagged to be accessible only on secure (HTTPS) sessions.
p. Browser cookies SHALL be accessible to the minimum practical set of hostnames and paths.
q. Expiration of browser cookies SHALL NOT be depended upon to enforce session timeouts.
r. The presence of an OAuth access token SHALL NOT be interpreted by the RP as presence of the subscriber, in the absence of other signals.

xviii. Session Reauthentication Requirements

a. Continuity of authenticated sessions SHALL be based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session
b. Session secrets SHALL be non-persistent, i.e., they SHALL NOT be retained across a restart of the associated application or a reboot of the host device.
c. Periodic reauthentication of sessions (at least every 12 hours per session) SHALL be performed to confirm the continued presence of the subscriber at an authenticated session.
d. A session SHALL NOT be extended past the guidelines in IA-5 o (2) a – j based on presentation of the session secret alone.
e. Prior to session expiration, the reauthentication time limit SHALL be extended by prompting the subscriber for the authentication factor(s) of a memorized secret or biometric.
f. If federated authentication is being used, then since the CSP and RP often employ separate session management technologies, there SHALL NOT be any assumption of correlation between these sessions.
g. An RP requiring reauthentication through a federation protocol SHALL — if possible, within the protocol — specify the maximum acceptable authentication age to the CSP.
h. If federated authentication if being used and an RP has specific authentication age requirements that it has communicated to the CSP, then the CSP SHALL reauthenticate the subscriber if they have not been authenticated within that time period.
i. If federated authentication is being used, the CSP SHALL communicate the authentication event time to the RP to allow the RP to decide if the assertion is sufficient for reauthentication and to determine the time for the next reauthentication event.

5.8.6 Authenticator Management – Authenticator Types

5.8.6.1 Memorized Secret Authenticators and Verifiers:

i. Maintain a list of commonly used, expected, or compromised passwords via API or download from a third party. Update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly. Compare current memorized secrets against the list quarterly.
ii. Require immediate selection of a new password upon account recovery.
iii. Allow user selection of long passwords and passphrases, including spaces and all printable characters.
iv. Employ automated tools to assist the user in selecting strong password authenticators.
v. If chosen by the subscriber, memorized secrets SHALL be at least 8 characters in length.
vi. If chosen by the CSP or verifier using an approved random number generator, memorized secrets SHALL be at least 6 characters in length.
vii. Truncation of the secret SHALL NOT be performed.
viii. Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant.
ix. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.
x. When processing requests to establish and change memorized secrets, SHALL verifiers compare the prospective secrets against the list maintained as required by NIST IA-5(1)(a)(1) that contains values known to be commonly used, expected, or compromised.

xi. If a chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret.
xii. If a chosen secret is found in the list, the CSP or verifier SHALL provide the reason for rejection.
xiii. If a chosen secret is found in the list, the CSP or verifier SHALL require the subscriber to choose a different value.
xiv. Verifiers SHALL implement a rate-limiting mechanism that effectively limits failed authentication attempts that can be made on the subscriber's account to no more than five.
xv. Verifiers SHALL force a change of memorized secret if there is evidence of compromise of the authenticator.
xvi. The verifier SHALL use approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.
xvii. The verifier SHALL use an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.
xviii. Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks.
xix. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function.
xx. The salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.
xxi. Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator
xxii. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be generated with an approved random bit generator of sufficient length.
xxiii. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL provide at least the minimum-security strength.
xxiv. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be stored separately from the memorized secrets.

5.8.6.2 Look-Up Secret Authenticators and Verifiers

i. CSPs creating look-up secret authenticators SHALL use an approved random bit generator to generate the list of secrets.
ii. Look-up secrets SHALL have at least 20 bits of entropy.
iii. If look-up secrets are distributed online, then they SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in IA-5 'n' 17 through 25.
iv. Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.
v. A given secret from an authenticator SHALL be used successfully only once
vi. If a look-up secret is derived from a grid (bingo) card, then each cell of the grid SHALL be used only once.
vii. Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks.
viii. If look-up secrets have at least 112 bits of entropy, then they SHALL be hashed with an approved one-way function

ix. If look-up secrets have less than 112 bits of entropy, then they SHALL be salted and hashed using a suitable one-way key derivation function.

x. If look-up secrets have less than 112 bits of entropy, then the salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.

xi. If look-up secrets have less than 112 bits of entropy, then both the salt value and the resulting hash SHALL be stored for each look-up secret.

xii. If look-up secrets that have less than 64 bits of entropy, then the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account.

xiii. The verifier SHALL use approved encryption when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.

xiv. The verifier SHALL use an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.

5.8.6.3 Out-of-Band Authenticators and Verifiers

i. The out-of-band authenticator SHALL establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request.

ii. Communication over the secondary channel SHALL be encrypted unless sent via the public switched telephone network (PSTN).

iii. Methods that do not prove possession of a specific device, such as voice-over-IP (VoIP) or email, SHALL NOT be used for out-of-band authentication.

iv. If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL uniquely authenticate itself by establishing an authenticated protected channel with the verifier.

v. If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL communicate with the verifier using approved cryptography.

vi. If PSTN is not being used for out-of-band communication, then the key used to authenticate the out-of-band device SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element).

vii. If the PSTN is used for out-of-band authentication and a secret is sent to the out-of-band device via the PSTN, then the out-of-band authenticator SHALL uniquely authenticate itself to a mobile telephone network using a SIM card or equivalent that uniquely identifies the device.

viii. If the out-of-band authenticator sends an approval message over the secondary communication channel, it SHALL either accept transfer of a secret from the primary channel to be sent to the verifier via the secondary communications channel, or present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant which it sends to the verifier.

ix. The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator.

x. Depending on the type of out-of-band authenticator, one of the following SHALL take place: transfer of a secret to the primary channel, transfer of a secret to the secondary channel, or verification of secrets by the claimant.

xi. If the out-of-band authenticator operates by transferring the secret to the primary channel, then the verifier SHALL transmit a random secret to the out-of-band authenticator and then wait for the secret to be returned on the primary communication channel.

xii. If the out-of-band authenticator operates by transferring the secret to the secondary channel, then the verifier SHALL display a random authentication secret to the claimant via the primary channel and then wait for the secret to be returned on the secondary channel from the claimant's out-of-band authenticator

xiii. If the out-of-band authenticator operates by verification of secrets by the claimant, then the verifier SHALL display a random authentication secret to the claimant via the primary channel, send the same secret to the out-of-band authenticator via the secondary channel for presentation to the claimant, and then wait for an approval (or disapproval) message via the secondary channel.

xiv. The authentication SHALL be considered invalid if not completed within 10 minutes.

xv. Verifiers SHALL accept a given authentication secret only once during the validity period.

xvi. The verifier SHALL generate random authentication secrets with at least 20 bits of entropy.

xvii. The verifier SHALL generate random authentication secrets using an approved random bit generator.

xviii. If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account.

xix. If out-of-band verification is to be made using the PSTN, then the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device.

xx. If out-of-band verification is to be made using the PSTN, then changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described above.

xxi. If PSTN is used for out-of-band authentication, then the CSP SHALL offer subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL.

xxii. If PSTN is used for out-of-band authentication, then the CSP SHALL Provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED.

xxiii. If PSTN is used for out-of-band authentication, then the CSP SHALL address any additional risk to subscribers in its risk assessment.

xxiv. If PSTN is used for out-of-band authentication, then the CSP SHALL develop a migration plan for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement.

5.8.6.4 OTP Authenticators and Verifiers

i. The secret key and its algorithm SHALL provide at least the minimum security strength of 112 bits as of the date of this publication.

ii. The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.

iii. OTP authenticators — particularly software-based OTP generators, SHALL NOT facilitate the cloning of the secret key onto multiple devices.

iv. The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy.
v. If the nonce used to generate the authenticator output is based on a real-time clock, then the nonce SHALL be changed at least once every 2 minutes.
vi. The OTP value associated with a given nonce SHALL be accepted only once.
vii. The symmetric keys used by authenticators are also present in the verifier and SHALL be strongly protected against compromise.
viii. If a single-factor OTP authenticator is being associated with a subscriber account, then the verifier or associated CSP SHALL use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output.
ix. The verifier SHALL use approved encryption when collecting the OTP.
x. The verifier SHALL use an authenticated protected channel when collecting the OTP.
xi. If a time-based OTP is used, it SHALL have a defined lifetime (recommended 30 seconds) that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP.
xii. Verifiers SHALL accept a given time-based OTP only once during the validity period.
xiii. If the authenticator output has less than 64 bits of entropy, the SHALL verifier implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).
xiv. If the authenticator is multi-factor, then each use of the authenticator SHALL require the input of the additional factor.
xv. If the authenticator is multi-factor and a memorized secret is used by the authenticator for activation, then that memorized secret SHALL be a randomly chosen numeric secret at least 6 decimal digits in length.
xvi. If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited.
xvii. If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.
xviii. If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an OTP has been generated.
xix. If the authenticator is multi-factor, the verifier or CSP SHALL establish, via the authenticator source, that the authenticator is a multi-factor device.
xx. In the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single factor.

5.8.6.5 Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based)

i. If the cryptographic authenticator is software based, the key SHALL be stored in suitably secure storage available to the authenticator application.
ii. If the cryptographic authenticator is software based, the key SHALL be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.
iii. If the cryptographic authenticator is software based, it SHALL NOT facilitate the cloning

of the secret key onto multiple devices.

iv. If the authenticator is single-factor and hardware-based, secret keys unique to the device SHALL NOT be exportable (i.e., cannot be removed from the device).

v. If the authenticator is hardware-based, the secret key and its algorithm SHALL provide at least the minimum-security length of 112 bits as of the date of this publication.

vi. If the authenticator is hardware-based, the challenge nonce SHALL be at least 64 bits in length.

vii. If the authenticator is hardware-based, approved cryptography SHALL be used.

viii. Cryptographic keys stored by the verifier SHALL be protected against modification.

ix. If symmetric keys are used, cryptographic keys stored by the verifier SHALL be protected against disclosure.

x. The challenge nonce SHALL be at least 64 bits in length.

xi. The challenge nonce SHALL either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator).

xii. The verification operation SHALL use approved cryptography.

xiii. If a multi-factor cryptographic software authenticator is being used, then each authentication requires the presentation of the activation factor.

xiv. If the authenticator is multi-factor, then any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret,

xv. If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited.

xvi. If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements including limits on the number of consecutive authentication failures.

xvii. If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an authentication transaction has taken place.

5.8.7 Authenticator Management – Public Key Based Authentication

5.8.7.1 For public key-based authentication:

i. Enforce authorized access to the corresponding private key.

ii. Map the authenticated identity to the account of the individual or group.

5.8.7.2 When public key infrastructure (PKI) is used:

i. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information.

ii. Implement a local cache of revocation data to support path discovery and validation

5.8.8 Authenticator Management – Protection of Authenticators

5.8.8.1 Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

5.8.9 Authenticator Management – Authentication Feedback

5.8.9.1 Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

5.8.10 Cryptographic Module Authentication

5.8.10.1 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

5.8.11 Identification and Authentication – Non Organizational Users

i. Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

ii. Identification and Authentication –Acceptance of PIV : Accept and electronically verify Personal Identity Verification-compliant credentials from other federal, state, local, tribal, or territorial (SLTT) agencies.

5.8.12 Identification and Authentication Acceptance of External Authenticators

i. Accept only external authenticators that are NIST-compliant.

ii. Document and maintain a list of accepted external authenticators.

5.8.13 Identification and Authentication – Non Organizational Users- Use of Defined Profiles

i. Conform to the following profiles for identity management: Security Assertion Markup Language (SAML) or OpenID Connect.

5.8.14 Re-Authentication

i. Require users to re-authenticate when: roles, authenticators, or credentials change, security categories of systems change, the execution of privileged functions occur, or every 12 hours.

5.8.15 Identity Proofing

i. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines.
ii. Resolve user identities to a unique individual.
iii. Collect, validate, and verify identity evidence.

5.8.16 Identity Proofing – Identity Evidence

i. Require evidence of individual identification be presented to the registration authority.

5.8.17 Identity Proofing – Identity Evidence Validation and Verification

i. Require that the presented identity evidence be validated and verified through agency-defined resolution, validation, and verification methods.
ii. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.
iii. Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context.
iv. Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification.
v. The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.
vi. If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively “identity service”), related fraud mitigation, or to comply with law or legal process, then CSPs SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing.
vii. If the CSP employs consent as part of its measures to maintain predictability and manageability, …then it SHALL NOT make consent for the additional processing a condition of the identity service.
viii. The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing.
ix. The CSP SHALL assess the [redress] mechanisms for their efficacy in achieving resolution of complaints or problems.
x. The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or practice statement that specifies the particular steps taken to verify identities.
xi. The practice statement SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled.

xii. The CSP SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the applicant as long as the identity exists in the information system.

xiii. The CSP SHALL record the types of identity evidence presented in the proofing process.

xiv. The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine:

xv. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein.

xvi. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply).

xvii. The schedule of retention for these records (Note: CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives

xviii. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.

xix. The entire proofing transaction, including transactions that involve a third party, SHALL occur over authenticated protected channels.

xx. If the CSP uses fraud mitigation measures, then the CSP SHALL conduct a privacy risk assessment for these mitigation measures. " Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented.

xxi. In the event a CSP ceases to conduct identity proofing and enrollment processes, then the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention.

xxii. The following requirements of CSP apply using the proofing service:

xxiii. The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers Privacy Act requirements.

xxiv. The agency SHALL publish a System of Records Notice (SORN) to cover such collection as applicable.

xxv. The agency SHALL consult with their SAOP to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers E-Government Act of 2002 requirements.

xxvi. The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collection as applicable.

xxvii. An enrollment code SHALL be comprised of one of the following:

- Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator.
- A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric.
- Enrollment code use has the additional requirement for code validity periods. The validity period is determined by the type of address where the enrollment code is sent, as follows:
- 10 days, when sent to a postal address of record within the contiguous United States.
- 30 days, when sent to a postal address of record outside the contiguous United States.
- 10 minutes, when sent to a telephone of record (SMS or voice).
- 24 hours, when sent to an email address of record.

xxviii. Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.

xxix. The CSP SHALL support in-person or remote identity proofing, or both.

- The CSP SHALL collect the following from the applicant:
- One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source.
- Two pieces of STRONG evidence.
- One piece of STRONG evidence plus two pieces of FAIR evidence.

5.9 Policy Area 9 – Incident Response

5.9.1 Incident Response Procedures

5.9.1.1 Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:

5.9.1.2 Agency-level incident response procedure that,

i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
iii. Facilitate the implementation of the incident response policy and the associated incident response controls.
iv. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures.
v. Review and update annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

5.9.2 Incident Response Training

5.9.2.1 Provide incident response training to system users consistent with assigned roles and responsibilities:

i. Prior to assuming an incident response role or responsibility or acquiring system access;
ii. When required by system changes.
iii. Annually thereafter.
iv. Review and update incident response training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
v. Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

5.9.3 Incident Response Testing

i. Test the effectiveness of the incident response capability for the system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency-appropriate tests
ii. Coordinate incident response testing with organizational elements responsible for related plans.

5.9.4 Incident Handling

i. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.
ii. Coordinate incident handling activities with contingency planning activities.
iii. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes; accordingly, and
iv. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.
v. Support the incident handling process using automated mechanisms (e.g., online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

5.9.5 Incident Monitoring

i. Track and document incidents.

5.9.6 Incident Reporting

i. All security incidents involving unauthorized access, data exposure, or potential breaches must be reported within 24 hours to CJIS-CT ISO, CSO. Agencies must document incident response plans and conduct annual table-top exercises
ii. Require personnel to report suspected incidents to the organizational response capability immediately but not to exceed one (1) hour after discovery.
iii. Report incident information to organizational personnel with incident handling responsibilities, and if confirmed, notify the CSO, SIB Chief, or Interface Agency Official.
iv. Report incidents using automated mechanisms.
v. Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

5.9.7 Incident Response Assistance

i. Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.
ii. Increase the availability of incident response information and support using automated mechanisms described in the discussion.

5.9.8 Incident Response Plan

5.9.8.1 Develop an incident response plan that:

i. Provides the organization with a roadmap for implementing its incident response capability.
ii. Describes the structure and organization of the incident response capability.
iii. Provides a high-level approach for how the incident response capability fits into the overall organization.
iv. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions.
v. Defines reportable incidents.
vi. Provides metrics for measuring the incident response capability within the organization.
vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability.
viii. Addresses the sharing of incident information.
ix. Is reviewed and approved by the organization's/agency's executive leadership annually.
x. Explicitly designates responsibility for incident response to CJIS-CT ISO.
xi. Distribute copies of the incident response plan to organizational personnel with incident handling responsibilities.
xii. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.
xiii. Communicate incident response plan changes to organizational personnel with incident handling responsibilities.
xiv. Protect the incident response plan from unauthorized disclosure and modification.

5.9.8.2 Include the following in the Incident Response Plan for breaches involving personally identifiable information.

i. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed.
ii. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms.
iii. Identification of applicable privacy requirements.

5.10 Policy Area 10 – Maintenance

5.10.1 Controlled Maintenance

i. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
ii. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location.
iii. Require that organizational personnel with information security and privacy responsibilities explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement.
iv. Sanitize equipment to remove information from associated media prior to removal from organizational facilities for off-site maintenance, repair, replacement, or destruction.
v. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions.
vi. Include the following information in organizational maintenance records:
   1. Component name
   2. Component serial number
   3. Date/time of maintenance
   4. Maintenance performed
   5. Name(s) of entity performing maintenance including escort if required.

5.10.2 Maintenance Tools

i. Approve, control, and monitor the use of system maintenance tools.
ii. Review previously approved system maintenance tools prior to each use.
iii. Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.
iv. Check media containing diagnostic and test programs for malicious code before the media are used in the system.
v. Prevent the removal of maintenance equipment containing organizational information by:
   a. Verifying that there is no organizational information contained on the equipment.
   b. Sanitizing or destroying the equipment.
   c. Retaining the equipment within the facility.
   d. Obtaining an exemption from organizational personnel with system maintenance responsibilities explicitly authorizing removal of the equipment from the facility.

5.10.3 Non Local Maintenance

i. Approve and monitor nonlocal maintenance and diagnostic activities.
ii. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system.
iii. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.
iv. Maintain records for nonlocal maintenance and diagnostic activities.
v. Terminate session and network connections when nonlocal maintenance is completed.

5.10.4 Maintenance Personnel

i. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.
ii. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations.
iii. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

5.10.6 Timely Maintenance

i. Obtain maintenance support and/or spare parts for critical system components that process, store, and transmit CJI within agency-defined recovery time and recovery point objectives of failure.

5.10.5 Patch Management

Patch Management policy establishes requirements for timely patching and vulnerability remediation of systems, applications, and devices to reduce exposure to known security vulnerabilities and maintain the confidentiality, integrity, and availability of organizational information systems in accordance with the FBI CJIS Security Policy and NIST Guidelines.

This policy applies to all organizational personnel, third-party contractors, and systems (servers, endpoints, mobile devices, network devices, applications, and cloud services) that process, store, or transmit organizational data.

The organization shall establish and maintain a documented patch management process to:

- Identify, evaluate, test, deploy, and verify patches and updates

- Prioritize patching based on asset criticality and risk exposure

- Integrate patching into the broader vulnerability management program

5.10.5.1 Patch Sources

- Approved sources for patches include software vendors, operating system providers, hardware manufacturers, and open-source project maintainers.

5.10.5.2 Patch Categories and Timelines

Patches must be applied according to the following priority levels, guided by guidelines and timelines.

Severity Level	Examples	Deployment Timeline
Critical	Exploited vulnerabilities, remote code execution, privilege escalation	Within 15 Days
High	Potential exploitation, security bypass, denial of service	Within 30 Days
Medium	Lesser impact vulnerabilities	Within 60 Days
Low	Minimal risk	Within 90 days

5.10.5.3 Patch Testing

- All patches must undergo testing in a controlled environment before deployment in production unless emergency remediation is warranted.

- Change Management Integration
- All patching activities must follow the organization's Change Management Policy, including documenting the patch, risk level, impact analysis, and approval.

- Vulnerability Identification
- Systems must be scanned regularly using vulnerability management tools (e.g., Tenable, Qualys, or Nessus).

- Vulnerabilities without vendor patches (zero-day) must be mitigated through compensating controls.

5.10.5.4 Emergency Patching

- For zero-day or critical vulnerabilities with active exploitation, emergency patching may bypass standard change approval with documented justification and notification to relevant stakeholders.

5.11 Policy Area 11 – Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and non-digital media in all forms is restricted to authorized individuals using authorized methods and processes. Procedures shall be defined for securely handling, transporting and storing media.

5.11.1 Media Access

CJIS-CT ISO shall securely store digital and non-digital media within physically secure locations or controlled areas.
CJIS-CT ISO shall restrict access to digital and non-digital media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted.
System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to hard copies of case file information stored in a locked filing cabinet is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media.

5.11.2 Media Storage

i. Physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible.
ii. Protect system media types defined until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

5.11.3 Media Transport

CJIS-CT ISO shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

i. Protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption. Physical media will be protected at the same level as the information would be protected in electronic form. Restrict the activities associated with transport of electronic and physical media to authorized personnel.
ii. Maintain accountability for system media during transport outside of the physically secure location or controlled areas.

iii. Document activities associated with the transport of system media.
iv. Restrict the activities associated with the transport of system media to authorized personnel.

5.11.3.1 Digital Media in Transit

“ Digital media” means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Controls shall be in place to protect Digital media containing State and CJI Data while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption is the optimal control during transport. However, if encryption of the data isn’t possible, each agency shall institute other controls to ensure the security of the data.

5.11.3.2 Non-Digital Media in Transit

The controls and security measures in this document also apply to State and CJI Data in non-digital (printed documents, printed imagery, etc.) form. non-digital media shall be protected at the same level as the information would be protected in electronic form.

5.11.4 Media Sanitization

i. Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration.
ii. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

5.11.5 Media Use

i. Restrict the use of digital and non-digital media on agency owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical, physical, or administrative controls (examples below).
ii. Prohibit the use of personally owned digital media devices on all agency owned or controlled systems that store, process, or transmit criminal justice information.
iii. Prohibit the use of digital media devices on all agency owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner.

5.12 Policy Area 12: Physical and Environmental Protection

Physical protection policy and procedures are to ensure State Data, CJI, Information system hardware, software, and media are physically protected through access control measures.

5.12.1 Review and update the current physical and environmental protection:

i. Policy annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI.
ii. Procedures annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI.

5.12.2 Physical and Environmental Protection - Physical Access Authorizations

i. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.
ii. Issue authorization credentials for facility access.
iii. Review the access list detailing authorized facility access by individuals annually and when personnel changes occur.
iv. Remove individuals from the facility access list when access is no longer required.

5.12.3 Physical and Environmental Protection - Physical Access Control

i. Enforce physical access authorizations by:
ii. Verifying individual access authorizations before granting access to the facility.
iii. Controlling ingress and egress to the facility using agency-implemented procedures and controls.
iv. Maintain physical access audit logs for the physically secure location and agency-defined sensitive areas.
v. Control access to areas within the facility designated as non-publicly accessible by implementing physical access devices including, but not limited to keys, locks, combinations, biometric readers, placards, and/or card readers.
vi. Escort visitors and control visitor activity in all physically secure locations.
vii. Secure keys, combinations, and other physical access devices.
viii. Inventory all agency-issued physical access devices annually.
ix. Change combinations and keys when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

5.12.4 Access Control for Transmission

Control physical access to information system distribution and transmission lines and devices within organizational facilities using agency-implemented procedures and controls.

5.12.5 Access Control for Output Devices

i. Control physical access to output from screens, monitors, printers, scanners, audio devices, facsimile machines, and copiers to prevent unauthorized individuals from obtaining the output.
ii. The agency shall control physical access to information system devices that display Criminal Justice Information (CJI) and shall position information systems devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

5.12.6 Monitoring Physical Access

i. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.
ii. Review physical access logs quarterly and upon occurrence of any physical, environmental, or security-related incidents involving CJI or systems used to process, store, or transmit CJI.
iii. Coordinate results of reviews and investigations with the organizational incident response capability.
iv. Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

5.12.7 Visitor Access Records

i. Maintain visitor access records to the facility where the system resides for one (1) year;
ii. Review visitor access records quarterly.
iii. Report anomalies in visitor access records to organizational personnel with physical and environmental protection responsibilities and organizational personnel with information security responsibilities.
iv. Limit personally identifiable information contained in visitor access records to the minimum PII necessary to achieve the purpose for which it is collected.

5.12.8 Power Equipment and Cabling

i. Protect power equipment and power cabling for the system from damage and destruction.
ii. Provide the capability of shutting off power to all information systems in emergency situations.
iii. Place emergency shutoff switches or devices in easily accessible locations to facilitate access for authorized personnel.
iv. Protect emergency power shutoff capability from unauthorized activation.
v. Provide an uninterruptible power supply to facilitate an orderly shutdown of the information system or transition of the information system to an alternate power source in

the event of a primary power source loss.

vi. Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

5.12.9 Fire Protection

i. Employ and maintain fire detection and suppression systems that are supported by an independent energy source.
ii. Employ fire detection systems that activate automatically and notify organizational personnel with physical and environmental protection responsibilities and police, fire, or emergency medical personnel in the event of a fire.

5.12.10 Environmental Controls

i. Maintain adequate HVAC levels within the facility where the system resides at recommended system manufacturer levels.
ii. Monitor environmental control levels continuously.
iii. Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

5.12.11 Delivery and Removal

i. Authorize and control information system-related components entering and exiting the facility.
ii. Maintain records of the system components.

5.12.12 Alternate Work Site

i. Determine and document all alternate facilities or locations allowed for use by employees.
ii. Employ the following controls at alternate work sites:
iii. Limit access to the area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
iv. Lock the area, room, or storage container when unattended.
v. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
vi. Follow the encryption requirements for electronic storage (i.e., data at-rest) of CJI.
vii. Assess the effectiveness of controls at alternate work sites.
viii. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

5.13 Policy Area 13: Planning

5.13.1 Develop security and privacy plans for the system that:

i. Are consistent with the organization's enterprise architecture.
ii. Explicitly define the constituent system components.
iii. Describe the operational context of the system in terms of mission and business processes.
iv. Identify the individuals that fulfill system roles and responsibilities.
v. Identify the information types processed, stored, and transmitted by the system.
vi. Provide the security categorization of the system, including supporting rationale.
vii. Describe any specific threats to the system that are of concern to the organization.
viii. Provide the results of a privacy risk assessment for systems processing personally identifiable information.
ix. Describe the operational environment for the system and any dependencies on or connections to other systems or system components.
x. Provide an overview of the security and privacy requirements for the system.
xi. Identify any relevant control baselines or overlays, if applicable.
xii. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions.
xiii. Include risk determinations for security and privacy architecture and design decisions.
xiv. Include security- and privacy-related activities affecting the system that require planning and coordination with organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities.
xv. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.
xvi. Distribute copies of the plans and communicate subsequent changes to the plans to organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities.
xvii. Review the security and privacy plans at least annually or when required due to system changes or modifications.
xviii. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments.
xix. Protect the plans from unauthorized disclosure and modification.

5.13.2 Rules of Behavior

i. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy.
ii. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system.
iii. Review and update the rules of behavior at least annually.
iv. Require individuals who have acknowledged a previous version of the rules of behavior to

read and re-acknowledge annually, or when the rules are revised or updated.

5.13.3 Rules of Behavior – Social Media and External Site/Application Usage Restrictions

5.13.3.1 Include in the rules of behavior, restrictions on:

i. Use of social media, social networking sites, and external sites/applications.
ii. Posting organizational information on public websites.
iii. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

5.13.4 System Security and Privacy Architectures

5.13.4.1 Develop security and privacy architectures for the system that:

i. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information.
ii. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals.
iii. Describe how the architectures are integrated into and support the enterprise architecture.
iv. Describe any assumptions about, and dependencies on, external systems and services.
v. Review and update the architectures at least annually or when changes to the system or its environment occur to reflect changes in the enterprise architecture.
vi. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

5.13.5 Central Management

The CJIS-CT Information Security Policy is centrally managed by the CJIS-CT ISO.

5.13.6 Baseline Selection

Select a control baseline for the system recommended in the CJIS-CT Security Policy.

5.13.7 Baseline Tailoring

Tailor the selected control baseline by applying specified tailoring actions.

5.14 Policy Area 14: Personnel Security

CJIS-CT shall carry out the following duties for the security of personnel who have access to CISS State and CJI Data in accordance with section 54-142i of the general statutes.

i. Agency-level personnel security policy that Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
ii. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls.
iii. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the personnel security policy and procedures.
iv. Review and update the current personnel security Policy annually and following assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

5.14.1 Position Risk Designation

i. Assign a risk designation to all organizational positions.
ii. Establish screening criteria for individuals filling those positions.
iii. Review and update position risk designations as required.

5.14.2 Personnel Screening – Applicable for CISS Search System

5.14.2.1Screen individuals prior to authorizing access to the CISS Search system.

i. To properly screen, state of residency and national fingerprint-based record checks shall be conducted. National fingerprint-based record checks must be conducted pursuant to an FBI approved authority such as a federal statute or a state statute approved pursuant to Public Law 92-544. If the person resides in a different state than that of the assigned agency, the agency shall also conduct state (of the agency) record checks. When appropriate, the screening shall be consistent with:
    a. 5 CFR 731.106.
    b. Office of Personnel Management policy, regulations, and guidance.
    c. agency policy, regulations, and guidance.
ii. Agencies authorized to bypass state repositories in compliance with federal law must only conduct a national fingerprint-based record check.
iii. Agencies without approved statutory authority authorizing or requiring civil fingerprint-based record checks on personnel with access to CHRI are exempt from this requirement until such time as appropriate statutory authority is obtained to conduct such record checks.
iv. All requests for access shall be made as specified by the CSO, Authorized Recipient Official, or IA Official. The CSO/designee, Authorized Recipient Official/designee, or IA Official is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency. All Authorized Recipient designees shall be employed

by the Authorized Recipient Agency.

v. If a criminal history record of any kind exists, access to CJI shall not be granted until the CSO/designee, Authorized Recipient Official/designee, or IA Official reviews the matter to determine if access is appropriate.
   a. If a felony conviction of any kind exists, the agency shall deny access to CJI. However, the requesting agency may ask for a review by the CSO/designee, Authorized Recipient Official/designee, or IA Official in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
   b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO/designee, Authorized Recipient Official/designee, or IA Official, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The requesting agency may request the CSO/designee, Authorized Recipient Official/designee, or IA Official review a denial of access determination.
   c. If a criminal history record of any kind is found on a contractor, the CA shall be formally notified of continuing fitness determination and system access shall be delayed pending review of the criminal history record information. The CA shall in turn notify the contractor's security officer.

vi. If the person appears to be a fugitive or has an arrest history without conviction, the CSO/designee, Authorized Recipient Official/designee, or IA Official shall review the matter to determine if access to CJI is appropriate.

vii. 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/designee, Authorized Recipient Official/designee, or IA Official. This does not implicitly grant hiring/firing authority with the CSA, Authorized Recipient, or IA Official only the authority to grant access to CJI. For offenses other than felonies, the CSO/designee, Authorized Recipient Official/designee, or IA Official has the latitude to delegate continued access determinations.

viii. If the CSO/designee, Authorized Recipient Official/designee, or IA Official determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.

ix. The criminal and non-criminal justice agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO/designee, Authorized Recipient Official/designee, or IA Official. and

x. Recommend rescreening individuals in accordance with the above. The authority authorized for the national fingerprint-based background check must also authorize the rescreening.

5.14.3 Personnel Screening for Contractors and Vendors

Contractors and vendors shall meet the following requirements:

i. To verify identification, state of residency and national fingerprint-based record checks shall be conducted 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). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with

a. 5 CFR 731.106
b. Office of Personnel Management policy, regulations, and guidance.
c. Agency policy, regulations, and guidance.

ii. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.

iii. 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.

a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.
c. If a record of any kind is found on a contractor, the CGA shall be formally notified, and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.
d. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.

iv. 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 to CJI is appropriate.

v. 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 CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.

vi. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied, and the person's appointing authority shall be notified in writing of the access denial.

vii. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI or physically secure locations or controlled areas (during times of CJI processing).

viii. Prior to granting access to State Data, the CGA, on whose behalf the Contractor is retained, shall verify identification of all personnel via a state of residency and national fingerprint-based record check. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks.

a. If a record of any kind is found, the CGA shall be formally notified, and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the Contractor-appointed Security Officer.
b. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the

authority to view CHRI) shall review the matter.

c. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
d. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
e. The CGA shall maintain a list of personnel who have been authorized access to State Data and shall, upon request, provide a current copy of the access list to the CJIS-CT ISO.
f. Applicants with a record of misdemeanor offense(s) may be granted access if the CJIS-CT ISO determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The CGA may request the CJIS-CT ISO to review a denial of access determination. It is recommended individual background investigations be conducted every five years, but it is not required.

ix. The policy does not require additional background investigations beyond the initial on current employees or contractors unless there is a break in service. A break in service is termination and then a subsequent rehire at a later date.

5.14.4 Personnel Termination

i. Disable system access Immediately.
ii. Terminate or revoke any authenticators and credentials associated with the individual.
iii. Conduct exit interviews that include a discussion of non-disclosure of CJI and PII.
iv. Retrieve all security-related organizational system-related property.
v. Retain access to organizational information and systems formerly controlled by terminated individuals.

5.14.5 Personnel Transfer

i. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization.
ii. Initiate appropriate actions such as closing and establishing accounts and changing system access authorizations within twenty-four (24) hours.
iii. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
iv. Notify organizational personnel with information security responsibilities, organizational personnel with personnel security responsibilities, system/network administrators, and organizational personnel with account management responsibilities prior to personnel transfer. Actions such as closing and establishing accounts or profiles and changing system access authorizations.

5.14.6 Access Agreements

i. Develop and document access agreements for organizational systems.

ii. Review and update the access agreements at least annually.
iii. Verify that individuals requiring access to organizational information and systems:
a. Sign appropriate access agreements prior to being granted access.
b. Re-sign access agreements to maintain access to organizational systems

5.14.7 External Personnel Security

i. Establish personnel security requirements, including security roles and responsibilities for external providers.
ii. Require external providers to comply with personnel security policies and procedures established by the organization.
iii. Document personnel security requirements.
iv. Require external providers to notify organizational personnel with information security responsibilities, organizational personnel with personnel security responsibilities, system/network administrators, or organizational personnel with account management responsibilities of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within twenty-four (24) hours.
v. Monitor provider compliance with personnel security requirements.

5.14.8 Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

i. Policy Reinforcement: Ensure policies clearly outline personnel responsibilities and consequences for violations.
ii. Incident Documentation: Maintain detailed records of incidents, sanctions applied, and remedial actions taken.
iii. Regular Audits and Compliance Checks: Continuously assess personnel adherence to CJIS-CT Security Policy.
iv. Sanction Gradation: Align sanctions with the severity of the violation and its impact on the agency's security posture.
v. Transparency and Appeal Process: Allow personnel an opportunity to appeal sanctions where appropriate, fostering fairness and accountability.

Severity	Severity Type	Sanction Type	Actions
Low	Minor or First-Time Violations	Verbal and Written Warnings	Document in personnel records for accountability.
		Mandatory Training or Remediation	Require personnel to complete additional security awareness or role-specific training.
Moderate	Repeated or Moderate Violations	Temporary Suspension of Access	Revoke access to CJI or systems temporarily for policy violations or pending investigation.
		Probation or Enhanced Monitoring	Place under close supervision with stricter oversight of CJI-related activities for a set period.
		Disciplinary Actions	Apply fines, formal reprimands, performance review penalties, or demotion for moderate breaches.
High	Serious or Repeated Violations	Revocation of Privileges or Roles	Remove personnel from roles involving CJI or critical systems for serious policy violations.
Critical	Severe Violations or Malicious Activities	Employment or Contract Termination	Terminate internal employees or contractors for intentional misuse, gross negligence, or severe breaches.
		Legal or Criminal Action	Initiate legal proceedings for malicious actions (e.g., theft, fraud) and report to law enforcement.
Organizational	Large number of violations	Contractual Penalties for Third Parties	Impose fines, terminate access, or cancel contracts for external providers violating compliance.
		Incident Reporting and Investigation	Establish protocols to document violations and ensure consistent sanctions are applied.

5.14.9 Position Descriptions

i. Incorporate security and privacy roles and responsibilities into organizational position descriptions.

5.15 Policy Area 15: Risk Assessment

5.15.1 Security Categorization

i. Categorize the system and information it processes, stores, and transmits.
ii. Document the security categorization results, including supporting rationale, in the security plan for the system.
iii. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

5.15.2 Risk Assessment

i. Conduct a risk assessment, including:
   a. Identifying threats to and vulnerabilities in the system.
   b. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information.
   c. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.
ii. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments.
iii. Document risk assessment results in a risk assessment report.
iv. Review risk assessment results at least quarterly.
v. Disseminate risk assessment results to organizational personnel with risk assessment responsibilities and organizational personnel with security and privacy responsibilities.
vi. Update the risk assessment at least quarterly or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

5.15.3 Vulnerability Monitoring and Scanning

i. Monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported.
   a. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for enumerating platforms, software flaws, and improper configurations.
   b. Formatting checklists and test procedures.
   c. Measuring vulnerability impact.
ii. Analyze vulnerability scan reports and results from vulnerability monitoring.
iii. Remediate legitimate vulnerabilities within the number of days listed.
   - Critical–15 days
   - High–30 days

- Medium–60 days
- Low–90 days.

iv. Share information obtained from the vulnerability monitoring process and control assessments with organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities to help eliminate similar vulnerabilities in other systems.

v. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

5.15.4 Vulnerability Monitoring and Scanning – Update Vulnerabilities to be scanned.

i. Update the system vulnerabilities to be scanned within 24 hours prior to running a new scan or when new vulnerabilities are identified and reported.

ii. Due to the complexity of modern software, systems, and other factors, new vulnerabilities are discovered on a regular basis. It is important that newly discovered vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner. The automated updates are available in the vulnerability scanner and not required to manually add.

5.15.5 Vulnerability Monitoring and Scanning – Privileged Access.

i. Implement privileged access authorization to information system components containing or processing CJI for vulnerability scanning activities requiring privileged access.

5.15.6 Vulnerability Monitoring and Scanning – Public Disclosure Program

i. Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

5.15.7 Risk Response

i. Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

5.15.8 Criticality Analysis

i. Identify critical system components and functions by performing a criticality analysis for information system components containing or processing CJI at the planning, design, development, testing, implementation, and maintenance stages of the system development life cycle.

5.16 Policy Area 16 : System and Service Acquisition

5.16.1 Allocation of Resources

i. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning.
ii. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process.

5.16.2 System Development Life Cycle

i. Acquire, develop, and manage the system using an agency documented system development lifecycle process that incorporates information security and privacy considerations.
ii. Define and document information security and privacy roles and responsibilities throughout the system development life cycle.
iii. Identify individuals having information security and privacy roles and responsibilities.
iv. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

5.16.3 Acquisition Process

Include the following requirements, descriptions, and criteria, explicitly or by reference, using agency defined contract language in the acquisition contract for the system, system component, or system service:

i. Security and privacy functional requirements.
ii. Strength of mechanism requirements.
iii. Security and privacy assurance requirements.
iv. Controls needed to satisfy the security and privacy requirements.
v. Security and privacy requirements.
vi. Requirements for protecting security and privacy documentation.
vii. Description of the system development environment and environment in which the system is intended to operate.
viii. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management.
ix. Acceptance criteria.
x. Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.
xi. Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes security-relevant external system interfaces; high-level design and a project plan that addresses sufficient detail to permit analysis and testing of the controls.
xii. Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.
xiii. Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

5.16.4 System Documentation

5.16.4.1 Obtain or develop administrator documentation for the system, system component, or system service that describes:

i. Secure configuration, installation, and operation of the system, component, or service.
ii. Effective use and maintenance of security and privacy functions and mechanisms.
iii. Known vulnerabilities regarding configuration and use of administrative or privileged functions.

5.16.4.2 Obtain or develop user documentation for the system, system component, or system service that describes,

i. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms.
ii. Methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner and protect individual privacy.
iii. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals.

5.16.4.3 Document steps to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent by contacting manufacturers, suppliers, or developers and conducting web-based searches in response.

5.16.4.4 Distribute documentation to organizational personnel with system and services responsibilities.'

5.16.5 Security and Privacy Engineering Principles

i. Apply agency documented systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components.
ii. Implement the privacy principle of minimization using only the Personally Identifiable Information necessary to perform system engineering.

5.16.6 External System Services

5.16.6.1 Require that providers of external system services comply with organizational security and privacy requirements and employ system and services acquisition security controls in accordance with the CJISSECPOL including the following agreements when applicable:

i. Management control agreement between CJIS-CT and the private organization.-

ii. Security Addendum: The CJIS-CT Security Addendum is a uniform addendum to an agreement between CJIS-CT and a private contractor, which specifically authorizes access to State and CJI data, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJISSECPOL provides for sanctions, and contains such other provisions as the Attorney General may require.

5.16.6.2 Private contractors designated to:

i. Perform criminal justice functions for a CJA.
ii. Perform criminal justice dispatching functions or data processing/information services for a NCJA (government), shall be eligible for access to State Data and CJI pursuant to an agreement which specifically identifies the private contractor's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJIS-CT and the private contractor shall incorporate the CJIS-CT Security Policy.
iii. Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by Government Agency performing a similar function and shall be subject to the same extent of audit review as are local user agencies.
iv. CJIS-CT employs the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis:
  a. All agencies having access to CJI shall permit an inspection team from CJIS-CT to conduct an appropriate inquiry and audit of any alleged security violations.
  b. CJIS-CT triennially audit all external service providers which have access to the information system in order to ensure compliance with applicable statutes, regulations, and policies.
  c. CJIS-CT has the authority to conduct unannounced security inspections and scheduled audits of external service providers' facilities.

5.16.6.3 CJIS-CT has the authority, on behalf of another CSA, to conduct a CJISSECPOL compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

5.16.6.4 CJIS-CT requires providers of the external system services to identify the functions, ports, protocols, and other services required for the use of such services: any system with a local network, or remote connection to an agency information system.

5.16.7 Developer Configuration Management

i. Require the developer of the system, system component, or system service to:
  a. Perform configuration management during system, component, or service during design, development, implementation, operation, and disposal.
  b. Document, manage, and control the integrity of changes to security configuration, network diagrams, and system components (hardware, software, firmware) by implementing access restrictions such as least privilege for changes.
  c. Implement only organization-approved changes to the system, component, or service.

d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes.
e. Track security flaws and flaw resolution within the system, component, or service and report findings to the individual(s) with information security responsibilities and an individual(s) with system and services acquisition responsibilities.

5.16.8 Developer Testing and Evaluation

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

i. Develop and implement a plan for ongoing security and privacy control assessments.
ii. Perform system and regression testing/evaluation at a level of comprehensive testing.
iii. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation.
iv. Implement a verifiable flaw remediation process.
v. Correct flaws identified during testing and evaluation.

5.16.9 Development Process, Standards, and Tools

i. Require the developer of the system, system component, or system service to follow a documented development process that:
    a. Explicitly addresses security and privacy requirements.
    b. Identifies the standards and tools used in the development process.
    c. Documents the specific tool options and tool configurations used in the development process.
    d. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development.
    e. Review the development process, standards, tools, tool options, and tool configurations to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy security and privacy requirements during design, development, implementation, operation, and disposal.
ii. Require the developer of the system, system component, or system service to perform a critical analysis:
    a. At the following decision points in the system development life cycle: design, development, implementation, and operational.
    b. At the following level of rigor: comprehensive testing.

5.16.10 Unsupported System Components

i. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.
ii. Provide the following options for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support.

5.17 Policy Area 17: System and communications protection.

Systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information.

5.17.1 Separation of System and User Functionality.

i. Separate user functionality, including user interface services, from system management functionality.

5.17.2 Information in shared resources

i. Prevent unauthorized and unintended information transfer via shared system resources.

5.17.3 Denial of Service Protection

i. Protect against or limit the effects of the following types of denial-of-service events: distributed denial of service, DNS Denial of Service, etc..
ii. Employ the following controls to achieve the denial-of-service objective: boundary protection devices and intrusion detection or prevention devices.

5.17.4 Boundary Protection

i. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.
ii. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks.
iii. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.
iv. Limit the number of external network connections to the system.
v. Implement a managed interface for each external telecommunication service.
vi. Establish a traffic flow policy for each managed interface.
vii. Protect the confidentiality and integrity of the information being transmitted across each interface.

viii. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need.

ix. Review exceptions to the traffic flow policy annually, after any incident, and after any major changes impacting the information system, while removing exceptions that are no longer supported by an explicit mission or business need.

x. Prevent unauthorized exchange of control plane traffic with external networks

xi. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks.

xii. Filter unauthorized control plane traffic from external networks.

xiii. Deny network communications traffic by default and allow network communications traffic by exception at boundary devices for information systems used to process, store, or transmit CJI.

xiv. Prevent split tunneling for remote devices connecting to organizational systems.

xv. Route all internal communications traffic that may be proxied, except traffic specifically exempted by organizational personnel with information security responsibilities, to all untrusted networks through authenticated proxy servers at managed interfaces.

xvi. Apply the following processing rules to data elements of personally identifiable information: all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

xvii. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system.

xviii. Document each processing exception.

xix. Review and remove exceptions that are no longer supported.

5.17.5 Transmission Confidentiality and Integrity

i. Protect the confidentiality and integrity of transmitted information.

ii. Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

iii. Implement cryptographic mechanisms to prevent unauthorized disclosure and detect unauthorized changes or access to CJI during transmission.

5.17.6 Network Disconnect

i. Terminate the network connection associated with a communications session at the end of the session or after one (1) hour of inactivity.

5.17.7 Cryptographic Protection

i. Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: encryption key generation, distribution, storage, access, and destruction is controlled by the agency.

ii. Determine the use of encryption for CJI in-transit when outside a physically secure location.

iii. Implement the following types of cryptography required for each specified cryptographic use: cryptographic modules which are Federal Information Processing Standard (FIPS)

140-3 certified, or FIPS validated algorithm for symmetric key encryption and decryption (FIPS 197 [AES]), with a symmetric cipher key of at least 128-bit strength for CJI in-transit.

5.17.8 Collaborative Computing Devices and Applications

i. Prohibit remote activation of collaborative computing devices and applications.
ii. Provide an explicit indication of use to users physically present at the devices.

5.17.9 Public Key Infrastructure Certificates

i. Issue public key certificates under an agency-level certificate authority or obtain public key certificates from an approved service provider.
ii. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

5.17.10 Mobile Code

i. Define acceptable and unacceptable mobile code and mobile code technologies.
ii. Authorize, monitor, and control the use of mobile code within the system.

5.17.11 Secure name/address resolution service (authoritative source)

i. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.
ii. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

5.17.12 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

i. Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

5.17.13 Architecture and Provisioning for Name/Address Resolution

i. Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

5.17.14 Session Authenticity

i. Protect the authenticity of communications sessions.

5.17.15 Protection of Information at Rest

i. Protect the confidentiality and integrity of the following information at rest: CJI when outside physically secure locations using cryptographic modules which are certified FIPS 140-3 with a symmetric cipher key of at least 128-bit strength, or FIPS 197 with a symmetric cipher key of at least 256-bit strength.

ii. Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

iii. The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g., government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e., United States, U.S. territories, Indian Tribes, and Canada) and are under legal authority of an APB-member agency (i.e., United States–federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police).

iv. Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on information systems and digital media outside physically secure locations: CJI.

5.17.16 Process Isolation

i. Maintain a separate execution domain for each executing system process.

5.18 Policy Area: 18 – System and Information Integrity (SI)

5.18.1 Flaw Remediation

i. Identify, report, and correct system flaws.
ii. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
iii. Install security-relevant software and firmware updates within the number of days listed after the release of the updates.
- Critical – 15 days
- High – 30 days
- Medium – 60 days
- Low – 90 days.

iv. Incorporate flaw remediation into the organizational configuration management process.
v. Determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools as least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI.

5.18.2 Malicious Code Protection

i. Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.
ii. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.
iii. Configure malicious code protection mechanisms to:

a. Perform periodic scans of the system at least daily and real-time scans of files from external sources at network entry and exit points and on all servers and endpoint devices as the files are downloaded, opened, or executed in accordance with organizational policy.
b. Block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures, send alert to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection. address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Solutions selected for deployment, whether locally installed or provided through a managed or external service arrangement, must demonstrate full adherence to CJIS-CT Security Policy and FBI CJIS Security Policy. This includes maintaining the confidentiality, integrity, and availability of State Data and CJI, supporting appropriate access controls, and undergoing appropriate configuration and monitoring. Document the implementation of such solutions and ensure that the service provider, where applicable, supports compliance with all applicable technical and administrative safeguards required by CJIS-CT Security Policy and FBI CJIS Security Policy.

5.18.3 System Monitoring

i. Monitor the system to detect attacks and indicators of potential attacks in accordance with the following monitoring objectives:

  a. Intrusion detection and prevention
  b. Malicious code protection
  c. Vulnerability scanning
  d. Audit record monitoring
  e. Network monitoring
  f. Firewall monitoring.

ii. Unauthorized local, network, and remote connections.

  a. Identify unauthorized use of the system through the following techniques and methods: event logging
  b. Invoke internal monitoring capabilities or deploy monitoring devices:
    - Strategically within the system to collect organization-determined essential information.
    - At ad hoc locations within the system to track specific types of transactions of interest to the organization.

iii. Analyze detected events and anomalies.
iv. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
v. Obtain legal opinion regarding system monitoring activities.
vi. Provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs to organizational personnel with information security responsibilities weekly.
vii. Employ automated tools and mechanisms to support near real-time analysis of logs and events. Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.
viii. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic.
ix. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions such as: the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information.

x. Alert organizational personnel with system monitoring responsibilities when the following system-generated indications of compromise or potential compromise occur: inappropriate or unusual activities with security or privacy implications.

xi. Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations in SI-4(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

5.18.4 Security Alerts, Advisories and Directives

i. Receive system security alerts, advisories, and directives from external source(s) (e.g., CISA, Multi-State Information Sharing & Analysis Center [MS-ISAC], U.S. Computer Emergency Readiness Team [USCERT], hardware/software providers, federal/state advisories, etc.) on an ongoing basis.

ii. Generate internal security alerts, advisories, and directives as deemed necessary.

iii. Disseminate security alerts, advisories, and directives to: organizational personnel implementing, operating, maintaining, and using the system.

iv. Implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.

5.18.5 Software, Firmware, and Information Integrity.

i. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information systems that contain or process CJI.

ii. Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate.

iii. Perform an integrity check of software, firmware, and information systems that contain or process CJI at agency-defined transitional states or security relevant events at least weekly or in an automated fashion.

iv. Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort.

v. Incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges.

vi. Discussion: Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

vii. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages.

viii. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

ix. System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions.

5.18.6 Spam Protection

i. Automatically update spam protection mechanisms at least daily.

ii. Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capabilities.

5.18.7 Information Input validation

i. Check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI. Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of “387,” “abc,” or “%K%” are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

5.18.8 Error Handlings

i. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.
ii. Reveal error messages only to organizational personnel with information security responsibilities.
iii. Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded. personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

5.18.9 Information Management and Retention

i. Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.
ii. Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative information.
iii. Limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected.
iv. Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for operational purposes helps to reduce the level of privacy risk created by a system. The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining which elements of personally identifiable information may create risk.
v. Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: data obfuscation, randomization, anonymization, or use of synthetic data.
vi. Organizations can minimize the risk to an individual's privacy by employing techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining the techniques to use and when to use them.

5.18.9.1Information Management and Retention | Information Disposal

i. Use the following techniques to dispose of, destroy, or erase information following the retention period:

a. Sanitize prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures.
b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
c. The disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.

5.18.10 Memory Protection

i. Implement the following controls to protect the system memory from unauthorized code execution: data execution prevention and address space layout randomization. Some adversaries launch attacks with the intent of executing code in nonexecutable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

5.19 Policy Area: 19 – Supply Chain Risk Management (SR)

5.19.1 Supply Chain Risk Management Plan

i. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: systems used to process, store, or transmit CJI.

ii. Review and update the supply chain risk management plan annually or as required, to address threat, organizational or environmental changes.

iii. Protect the supply chain risk management plan from unauthorized disclosure and modification.

iv. Establish a supply chain risk management team consisting of individuals with security responsibilities and supply chain risk management responsibilities to lead and support the following SCRM activities: information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions.

5.19.2 Acquisition Strategies, Tools, and Methods

i. All third-party vendors handling CJI data must undergo an annual security assessment, including penetration testing and compliance review. Contracts must include data protection clauses aligned with FBI CJIS standards

5.19.3 Notification Agreements

i. Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises to systems sent to process, store, or transmit CJI.

5.19.4 Evaluation, Security testing and Inspection of Systems or Components

i. Evaluate, perform security testing and Inspect the systems or system components upon initial procurement and periodically as needed to detect tampering: systems used to process, store, or transmit CJI.

5.19.5 Component Disposal

i. Dispose of CJI using the techniques and methods as described in Media Protection.

5.20 Policy Area 20: Mobile Devices

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

CJIS-CT shall,

i. Establish usage restrictions and implementation guidance for mobile devices accessing State Data and CJI.
ii. Authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

5.20.1 Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and based upon the specific technology or implementation; wireless technologies may require additional security controls as described below.

5.20.1.1 802.11 Wireless Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

i. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
ii. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
iii. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
iv. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
v. Enable user authentication and encryption mechanisms for the management interface of the AP.
vi. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with the password requirements.
vii. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.
viii. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID

feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.

ix. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
x. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
xi. Ensure that the ad hoc mode has been disabled.
xii. Disable all nonessential management protocols on the APs.
xiii. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g., SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
xiv. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum, logs shall be reviewed monthly.
xv. Insulate, virtually (e.g., virtual local area network (VLAN) and ACLs) or physically (e.g., firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
xvi. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.20.1.2 Cellular Devices

i. Cellular telephones, smartphones (i.e., Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and “aircards” are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

5.20.1.3 Cellular Service Abroad

i. Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a “trusted” entity by the device.
ii. When devices are authorized to access information outside the U.S., CJIS-CT shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the policies prior to and after deployment outside of the U.S.

5.20.1.4 Voice Transmissions Over Cellular Devices

i. Any cellular device used to transmit State Data and CJIS Information via voice is exempt from the encryption and authentication requirements.

5.20.1.5 Bluetooth

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g., denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. CJIS-CT security policy shall be used to dictate the use of Bluetooth and its associated devices based on the CJIS-CT's operational and business processes.

5.20.1.6 Mobile Hotspots

Many mobile devices include the capability to function as a Wi-Fi hotspot that allows other devices to connect through the device to the internet over the device's cellular network.

When CJIS-CT allows mobile devices that are approved to access or store Information to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

i. Enable encryption on the hotspot
ii. Change the hotspot's default SSID
iii. Ensure the hotspot SSID does not identify the device make/model or agency ownership
iv. Create a wireless network password (pre-shared key)
v. Enable the hotspot's port filtering/blocking features if present
vi. Only allow connections from agency-controlled devices

5.20.2 Mobile Device Management (MDM)

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit data at any time. User agencies shall implement the following controls when directly accessing data from devices running a limited-feature operating system:

i. Ensure that information is only transferred between CJIS-CT authorized applications and storage areas of the device.
ii. MDM with centralized administration configured and implemented to perform at least the following controls:
   a. Remote locking of device
   b. Remote wiping of device
   c. Setting and locking device configuration
   d. Detection of “rooted” and “jailbroken” devices
   e. Enforcement of folder or disk level encryption
   f. Application of mandatory policy settings on the device
   g. Detection of unauthorized configurations
   h. Detection of unauthorized software or applications
   i. Ability to determine the location of agency-controlled devices
   j. Prevention of unpatched devices from accessing CJIS-CT systems/information.
   k. Automatic device wiping after a specified number of failed accesses attempts

5.20.3 Wireless Device Risk Mitigations

CJIS-CT shall ensure that wireless devices accessing CJIS-CT information

i. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.
ii. Are configured for local device authentication (see Section 5.13.7.1).
iii. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.
iv. Encrypt all CJIS-CT Information resident on the device.
v. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
vi. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
vii. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

5.20.4 System Integrity

CJIS-CT shall implement the requirements of Section 5.10 of the CJIS-CTSecurity Policy with the installation of a third-party MDM, application, or supporting service infrastructure.

i. Patching/Updates: CJIS-CT shall implement systems to monitor mobile devices to ensure their patch and update state is current.
ii. Malicious Code Protection: CJIS-CT shall implement a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without an MDM solution is acceptable under this section.
iii. Personal Firewall: CJIS-CT shall implement personal firewall to be employed on all mobile devices that have a full-feature operating system (i.e., laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

    a. Manage access to the Internet program.
    b. Block unsolicited requests to connect to the user device.
    c. Filter incoming traffic by IP address or protocol.
    d. Filter incoming traffic by destination ports.
    e. Maintain an IP traffic log.

Mobile devices with limited-feature operating systems (i.e., tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full-feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

5.20.5 Incident Response

CJIS-CT shall implement additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

i. Loss of device control. For example:

   a. Device known to be locked, minimal duration of loss.
   b. Device lock state unknown, minimal duration of loss
   c. Device lock state unknown, extended duration of loss
   d. Device known to be unlocked, more than momentary duration of loss.

ii. Total loss of device

   a. Device compromise
   b. Device loss or compromise outside the United States

5.20.6 Access Control

i. Multiple user accounts are not generally supported on limited-feature mobile operating systems. Access control shall be accomplished by the application that accesses CJIS-CT Information.

5.20.7 Identification and Authentication

ii. Due to the technical methods used for identification and authentication on many limited-feature mobile operating systems, achieving compliance may require many different components.

5.20.7.1 Local Device Authentication

i. When mobile devices are authorized for use in accessing CJIS-CT information, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.

5.20.7.2 Advanced Authentication

i. When accessing CJIS-CT information from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described. If access is indirect, then AA is not required.

5.20.8 Compensation Controls

CJIS-CT approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited-feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints.
Mobile Device Management (MDM) shall be implemented. The compensating controls shall:

i. Meet the intent of the CJIS-CT Security Policy AA requirement
ii. Provide a similar level of protection or security as the original AA requirement
iii. Not rely upon the existing requirements for AA as compensating controls
iv. Expire upon the CSO approved date or when a compliant AA solution is implemented.

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls. The compensating controls for AA are a combination of controls providing acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

The following minimum controls shall be implemented as part of the CSO approved compensating controls:

- Possession and registration of an agency issued smartphone or tablet as an indication it is the authorized user
- Use of device certificates
- Implemented CJIS-CT Security Policy compliant standard authenticator protection on the secure location where CJI is stored.

5.20.9 Device Certificates

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.
When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

i. Protected against being extracted from the device
ii. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts

6. APPENDIX A: Terms and Definitions

1. 28 CFR Certification Indicator — True if the user has been trained and certified in the handling of criminal intelligence data in accordance with Code of Federal Regulations Title 28 (28 CFR) Part 23, false otherwise. Usage information: Assertion of this privilege requires the user to have been trained and certified in the handling of criminal intelligence data in accordance with Code of Federal Regulations Title 28 (28 CFR) Part 23. One way for a user to meet this requirement is by having taken and passed the online 28 CFR Part 23 training course and certification exam offered by the U.S. Department of Justice Bureau of Justice Assistance (BJA) via its Secured National Criminal Intelligence Resource Center (NCIRC) Web Site (http://www.ncirc.gov/securedwebsite.cfm). Alternatively, a user may meet this requirement by having taken and passed an equivalent offline 28 CFR Part 23 training course, offered by the Institute for Intergovernmental Research (IIR). (See https://28cfr.iir.com/ for details.)
2. Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.
3. Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information and criminal justice employment. In addition, administration of criminal justice includes "crime prevention programs" to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g., record checks of individuals who participate in Neighborhood Watch or "safe house" programs) and the result of such checks will not be disseminated outside the law enforcement agency.
4. Agency Controlled Mobile Device — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJI. The device can be agency issued or BYOD (personally owned).
5. Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.
6. Agency Issued Mobile Device — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJI. The device is not BYOD (personally owned).
7. Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS-CT systems agency, there is no requirement for the appointment of an agency liaison.
8. Asymmetric Encryption — A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.
9. Authenticator Assurance Level — The authenticator assurance level as defined by NIST SP 800-63-3. There are three defined levels: AAL1 (low), AAL2 (medium), and AAL3 (high). Usage information: IDPs should assert this attribute to indicate the strength of the authenticator

used for the current authentication process; AAL1 (low), AAL2 (medium), and AAL3 (high). AAL2 and AAL3 require multifactor authentication; although the use of multiple factors does not automatically qualify for AAL2.

10. Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.
11. Authorized Recipient (AR) — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes. (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
12. Authorized Recipient Security Officer (ARSO) the individual appointed by the AR to coordinate and oversee Information Security by ensuring that the Channeler is adhering to the CJISSECPOL and Outsourcing Standard, verifying the completion of annual Security Awareness Training, and communicating with the FBI CJIS Division on matters relating to Information Security.
13. Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.
14. Basic Testing — A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as black box testing.
15. Comprehensive Testing — A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing.
16. Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.
17. Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.
18. Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regard to CJI, it is the information about the history of criminal incidents.
19. Certificate Authority (CA) Certificate — Digital certificates required for certificate-based authentication that are issued to tell the client computers and servers that it can trust other certificates that are issued by this CA.
20. Channeler — A FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.
21. Cloud Client — A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

22. Cloud Computing — A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.
23. Cloud Provider — An organization that provides cloud computing services.
24. Cloud Subscriber — A person or organization that is a customer of a cloud computing service provider.
25. CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.
26. CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the FBI CJIS Security Policy.
27. CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.
28. CJIS-CT Information Security Officer (CJIS-CT ISO) - The appointed CJIS-CT personnel responsible to coordinate information security efforts at CJIS-CT.
29. CJIS Systems Officer (CSO) - The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.
30. Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.
31. Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.
32. Compensating Controls — Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must meet the intent of the FBI CJIS Security Policy AA requirement Provide a similar level of protection or security as the original AA requirement Not rely upon the existing requirements for AA as compensating controls.

    Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.
33. Computer Security Incident Response Capability (CSIRC) - A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.
34. Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.
35. Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal

Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

36. Contracting Government Agency (CGA) The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.
37. Controlled Unclassified Information (CUI) Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. (32 CFR Vol 6 Part 2002)
38. Counter Terrorism Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for counter-terrorism data and documents within the user's home system, network, or agency. False otherwise. Usage information: Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.
39. Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.
40. Criminal History Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for criminal history data and documents within the user's home system, network, or agency. False otherwise. Usage information: Example data sources include National Crime Information Center (NCIC) Criminal History. User eligibility requirements are decided by federation members but may include Fingerprint (FP) based background, NCIC training, access to Law Enforcement criminal history data in home agency, member of agency with Law Enforcement Originating Agency (ORI) code. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.
41. Criminal History Record Information (CHRI) Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information's, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.
42. Criminal Intelligence Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for criminal intelligence data and documents within the user's home system, network, or agency. False otherwise. Usage information: Example data sources include Criminal Law Enforcement Reporting Information System (CLERIS), Regional Information Sharing Systems (RISS), Joint Regional Information Exchange System (JRIES), and Law Enforcement Intelligence Units (LEIU). User eligibility requirements are decided by federation members but may include: 28 CFR (23) training, Fingerprint (FP) based background, access to intelligence data in home agency, member of agency with Law Enforcement Originating Agency (ORI) code. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.
43. Criminal Investigative Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency)

for criminal investigative data and documents within the user's home system, network, or agency. False otherwise. Usage information: Example data sources include Criminal Law Enforcement Reporting Information System (CLERIS) and Contact and Information Management System (CIMS). User eligibility requirements are decided by federation members, but may include: Fingerprint (FP) based background, access to investigative data in home agency, member of agency with Law Enforcement Originating Agency (ORI) code. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

44. Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.
45. Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.
46. Criminal Justice Conveyance — A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.
47. Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the 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.
48. Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g., solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.
49. Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.
50. Digital Media — Any form of electronic media designed to store data in a digital format. This includes but is not limited to: memory device in laptops, computers, and mobile devices and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.
51. Digital Signature — A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying

algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key to convert encrypted information back into a plaintext (readable) format.

52. Direct Access (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.
53. Display Name — The user's display name is a text string formatted for display purposes in applications and correspondence.
54. Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.
55. Email Address Text — The electronic mailing address by which the user may be contacted.
56. Employer Name — The name of the organization that is the user's primary employer.
57. Employer ORI — A unique identifier assigned to the organization that is the user's primary employer. ORIs are generally assigned by the FBI; however, in some cases they may be assigned by other agencies.
58. Employer Organization General Category Code —The general category of the organization that is the user's primary employer.
59. Employer State Code — The state, commonwealth, province, or other such geopolitical subdivision of the country in which is located the primary business office of the organization that is the user's primary employer.
60. Encryption — A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.
61. Escort — Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.
62. Facsimile (Fax) — Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.
63. Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.
64. FBI CJIS Information Security Officer (FBI CJIS ISO) The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.
65. FBI CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI

CJIS ISO; the document containing this glossary.

66. Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
67. Federation Assurance Level — There are 3 Federation Assurance Levels representing the assurance level of the user's federated assertion: FAL1 (low assurance), FAL2 (moderate assurance), and FAL3 (high assurance) based on NIST SP 800-63-3. Usage information: IDPs should assert this for all assertions sent to RPs correctly identifying the level of assurance of the assertion. The RP can also derive the FAL if not asserted.
68. Federation Id — The persistent, federation-unique identifier for the user, comprising a federation part, an optional trusted identity broker (TIB) part, an identity provider (IDP) part, and a local ID.
69. Focused Testing — A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as gray box testing.
70. For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.
71. Full-feature Operating System — Full-feature operating systems are traditional operating systems used by a standard desktop computer (e.g., Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). These operating systems are generally open to user control and configuration and therefore require configuration management to properly secure, or “harden”, these devices from malicious network based technical attacks (e.g., malware, spyware, hackers, etc.). These operating systems require traditional protection applications such as antivirus programs and personal firewalls.
72. General User — A user, but not a process, who is authorized to use an information system.
73. Given Name — The first name of the user.
74. Government Data Self Search Home Privilege Indicator — True if the user has permission to search on behalf of himself/herself (NOT on behalf of the user's home agency) for government data and documents within the user's home system, network, or agency. False otherwise. Usage information: Example data sources include Tax Data, Labor Data, Uniform Commercial Code (UCC) Filings, Property Records, Department of Motor Vehicles (DMV), Drivers License (DL), Boat Ownership, Corporate Records, and Protected Critical Infrastructure Information (PCII). User eligibility requirements are decided by federation members, but may include: Agency vetting, application training, state law, and Federal law. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.
75. Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtual machine (VM).
76. Hashing — The process of applying a mathematical algorithm to data to produce an alphanumeric value (i.e., hash value) to be used as a representative of that data.
77. Hash Value — The term that refers to an alphanumeric value which represents the result of

applying a cryptographic hash function to data.

78. Host Operating System — In the context of virtualization, the operating system that interfaces with the actual physical hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

79. Hybrid Encryption — A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution, the asymmetric encryption keys are used for client/server certificate exchange to provide session
80. integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

81. Hypervisor — See Host Operating System.

82. Identity Assurance Level — The maximum NIST identity assurance level as defined by NIST SP 800-63-3 for which the identity proofing process of this Identity Provider Organization qualifies. There are three defined levels: IAL1 (low), IAL2 (medium), and IAL3 (high). Usage information: IDPs should use this attribute to indicate the assurance level of their identity and attribute proofing processes.

83. Identity History Data — Textual data corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

84. Identity Provider Id — The unique identifier within the federation that identifies the identity provider (IDP) of the user within the federation. Comprises a federation part, an optional trusted identity broker (TIB) part, and an identity provider (IDP) part. The general format of an identity provider ID is: “Federation}:[TIB:{TIB}:]IDP:{IDP}". Usage information: This identifier MUST be consistent with the federation identifier, IDP identifier, and (if applicable) TIB identifier denoted within the user's Federation Id attribute.

85. In-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.

86. Indirect Access — Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g., CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

87. Information — See data and CJI.

88. Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party’s information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

89. Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

90. Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

91. Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint

and criminal history system maintained by the FBI CJIS Division that provides the law
92. enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

93. Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.
94. Intelligence Analyst Indicator — True if the user is an Intelligence Analyst (IA) for a government agency, false otherwise. Usage information: An Identity Provider (IdP) may assert that a user is an IA if they work for a government agency, and/or company who works with the government, in order to provide information assessments about criminal or security threats.
95. Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.
96. Interface Agency — A criminal justice agency (including law enforcement) or any federally authorized agency/entity, other than a CSA or State Identification Bureau (SIB), that leverages a direct connection to the FBI CJIS Division.
97. Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.
98. Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.
99. Intrusion Detection — The process of monitoring the events occurring in an information system or network and analyzing them for signs of possible incidents.
100. Intrusion Detection System — Software which automates the intrusion detection process.
101. Intrusion Prevention — The process of monitoring events occurring in an information system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.
102. Intrusion Prevention System — Software which has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.
103. Jailbreak (Jailbroken) — The process of attaining privileged control (known as "root access") of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.
104. Laptop Devices — Laptop devices are mobile devices with a full-featured operating system (e.g., Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g., smartphones), or mobile devices that feature a limited-feature operating system (e.g., tablets).
105. Law Enforcement Enterprise Portal (LEEP) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate

on FOUO matters.

106. Limited-feature Operating System — Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g., Apple iOS, Android, Windows Mobile, Blackberry OS, etc.). There operating systems permit limited user control but are inherently more resistant than a full-feature operating system to certain types of network based technical attacks due to the limited-feature sets. Devices using these operating systems are required to be managed by a mobile device management solution.
107. Local Id — The unique local identifier associated with the user for internal purposes within the user's identity provider (IDP). This identifier is assigned and maintained by a federation member agency or partner organization and used for local authentication and identification. The identifier typically has local significance and is integrated into the existing legacy IT infrastructure and/or business processes of the federation member agency or partner organization.
108. Logical Access — The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.
109. Logical Partitioning — When the host operating system, or hypervisor, allows multiple guest operating systems to share the same physical resources.
110. Local Agency Security Officer (LASO) The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.
111. Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA's authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.
112. Metadata — Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is commonly referred to as data about data, information about information, or information describing the characteristics of data.
113. Mobile Device — Any portable device used to access CJI via a wireless connection (e.g., cellular, Wi-Fi, Bluetooth, etc.).
114. Mobile Device Management (MDM) Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets.
115. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.
116. Mobile (Wi-Fi) Hotspot — A mobile (Wi-Fi) hotspot is a zone or area associated with a mobile device (e.g., smartphone, air card) allowing wireless connectivity to the Internet typically

through a cellular connection.

117. National Crime Information Center (NCIC) — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.
118. National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.
119. National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.
120. Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
121. NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.
122. NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a local bank.
123. NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a county school board which uses CHRI to assist in employee hiring decisions.
124. NCIC Certification Indicator — True if the user has a valid, active certification in the usage and handling of data in accordance with National Crime Information Center (NCIC) rules and regulations, false otherwise.
125. N-DEx Privilege Indicator — True if the user has privileges to access the Federal Bureau of Investigation (FBI) Law Enforcement National Data Exchange (N-DEx), false otherwise. Usage information: Assertion of this privilege requires the user to meet certain requirements which are not currently documented in the GFIPM Metadata Specification. Future versions of this spec will properly document these requirements. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.
126. Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
127. Non-digital Media — Non-digital media means a hard copy or physical representation of information, including, but not limited to, paper copies, printer ribbons, drums, microfilm, platens, and other forms of preserved or preservable information.
128. Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the supervision of other Executive Branch agencies, and to oversee and coordinate the

Presidential Administration's procurement, financial management, information, and regulatory policies.

129. One-time Password — A disposable, single-use standard authenticator for access CJI. One-time passwords are: minimum of six (6) randomly generated characters, valid for a single session, and if not used, expire within a minimum of five (5) minutes after issuance.
130. 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 CJISSECPOL.
131. Out-of-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.
132. Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.
133. Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.
134. Partitioning — Managing guest operating system, or virtual machine, access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest operating systems resources or any resources not allocated for virtualization use.
135. Password Verifier (Verifier) — An entity or process that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.
136. PCII Certification Indicator — True if the user has a valid, active certification in the usage and handling of Protected Critical Infrastructure Information (PCII) data in accordance with US Department of Homeland Security (DHS) rules and regulations, false otherwise. Usage information: Information about PCII authorized user training is available at the following URL. http://www.dhs.gov/receive-pcii-authorized-user-training
137. Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.
138. Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an 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 as date and place of birth, or mother's maiden name.
139. Physical Access — The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g., the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).
140. Physical Media — Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.
141. Physical Partitioning — When the host operating system, or hypervisor, assigns separate physical resources to each guest operating systems, or virtual machine.
142. Physically Secure Location — A facility, a criminal justice conveyance, 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.

143. Pocket/Handheld Mobile Device — Pocket/Handheld mobile devices (e.g., smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.
144. Privileged User — A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform.
145. Property Data — Information about vehicles and property associated with a crime.
146. Public Safety Officer Indicator — True if the user is a public safety officer (PSO), false otherwise. Usage information: An IDP may assert that a user is a PSO if the user is authorized to act in a role pursuant to the safety and welfare of the public within a government jurisdiction. This may include firefighters, emergency medical technicians (EMTs), hazardous materials (HAZMAT) cleanup specialists, etc.
147. Rap Back — Record of Arrest and Prosecution Back. A NGI service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.
148. Receive-Only Terminal (ROT) — A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).
149. Repository Manager, or Chief Administrator — The designated manager of the agency having oversight responsibility for a CSA's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.
150. Root (Rooting, Rooted) — The process of attaining privileged control (known as "root access") of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.
151. Salting — The process of applying a non-secret value to data prior to applying a cryptographic process, such as hashing. This process changes the value to be hashed in a manner designed to ensure an attacker cannot reuse the results of computations for one instance.
152. Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.
153. Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.
154. Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g., SSI, CII)

while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

155. Server/Client Computer Certificate (device-based) — Digital certificates that are issued to servers or client computers or devices by a CA and used to prove device identity between server and/or client computer devices during the authentication process.
156. Service — The organized system of apparatus, appliances, personnel, etc., that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.
157. Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.
158. Smartphone — See pocket/handheld mobile devices.
159. Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.
160. Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.
161. State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.
162. State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
163. State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.
164. State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.
165. State of Residency — A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. CJIS Systems Officers have the latitude to determine what documentation constitutes acceptable proof of residency.
166. Sur Name — The last name or family name of the user.
167. Sworn Law Enforcement Officer Indicator — True if the user is a sworn law enforcement

officer (SLEO), false otherwise. Usage information: An IDP may assert that a user is a SLEO if all of the following conditions are true. The user is a full-time employee of a state-recognized law enforcement agency. The user is authorized (has the authority) to make an arrest. The user is certified by a State Certifying Authority (i.e., Peace Officer Standards and Training (POST)), or equivalent.

168. Alternatively, an IDP may assert that a user is a SLEO if the user is a full time employee of a state-recognized law enforcement agency, acting on behalf of a SLEO, in performance of the user's assigned duties. Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.
169. Symmetric Encryption — A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.
170. System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to applications and all interconnecting infrastructure required to use those applications that process CJI.
171. Tablet Devices — Tablet devices are mobile devices with a limited-feature operating system (e.g., iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g., smartphones) or mobile devices with full-featured operating systems (e.g., laptops).
172. Telephone Number — The telephone number for a telecommunication device by which the user may be contacted.
173. Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.
174. Unique Subject Id — A persistent unique identifier for the subject or user that identifies both the subject or user and their identity provider. The identity provider should be identified by a fully qualified domain name.
175. User Certificate (user-based) — Digital certificates that are unique and issued to individuals by a CA. Though not always required to do so, these specific certificates are often embedded on smart cards or other external devices as a means of distribution to specified users. This certificate is used when individuals need to prove their identity during the authentication process.
176. Virtual Escort — Authorized personnel who actively monitor a remote maintenance session on Criminal Justice Information (CJI)-processing systems. The escort must have the ability to end the session at any time deemed necessary to ensure the protection and integrity of CJI at all times.
177. Virtual Machine (VM) — See Guest Operating System
178. Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.
179. Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

180. Wireless Access Point — A wireless access point is a device that logically connects a wireless client device to an organization's enterprise network which processes unencrypted CJI.
181. Wireless (Wi-Fi) Hotspot — A wireless (Wi-Fi) hotspot is a zone or area within a fixed location allowing wireless connectivity to the Internet typically through a wired connection. Hotspots are typically available in public areas such as airports, hotels and restaurants.

7. APPENDIX B: Acronyms

AA	Advanced Authentication
AAL	Authentication Assurance Level
AAL1	Authentication Assurance Level 1
AAL2	Authentication Assurance Level 2
AAL3	Authentication Assurance Level 3
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CISA	Cybersecurity & Infrastructure Security Agency
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
CSP	Credential Service Provider
CUI	Controlled Unclassified Information
DAA	Designated Approving Authority
DoJ	Department of Justice
DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer

IT	Information Technology
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LMR	Land Mobile Radio
MAC	Media Access Control
MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle
MOU	Memorandum of Understanding
MS-ISAC	Multi-State Information Sharing & Analysis Center
NARA	National Archives and Records Administration
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OTP	One-time Password
PBX	Private Branch Exchange
PCSC	Preventing and Combating Serious Crime
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RCMP	Royal Canadian Mounted Police
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau
SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TSC	Threat Screening Center
TLS	Transport Layer Security
UCN	Universal Control Number
USCERT	U.S. Computer Emergency Readiness Team
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy

WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

8. APPENDIX C: Network Topology Drawings

1. CJIS-CT Network Drawing - Confidential
   (Please reach out to CJIS-CT ISO for the sample Agreements/MOUs)

9. APPENDIX D: Sample Agreements/MOUs

i MOU – New Agency onboarding
ii MOU - For sharing Information/Databases
iii MOU - Federation of Identity Management Systems

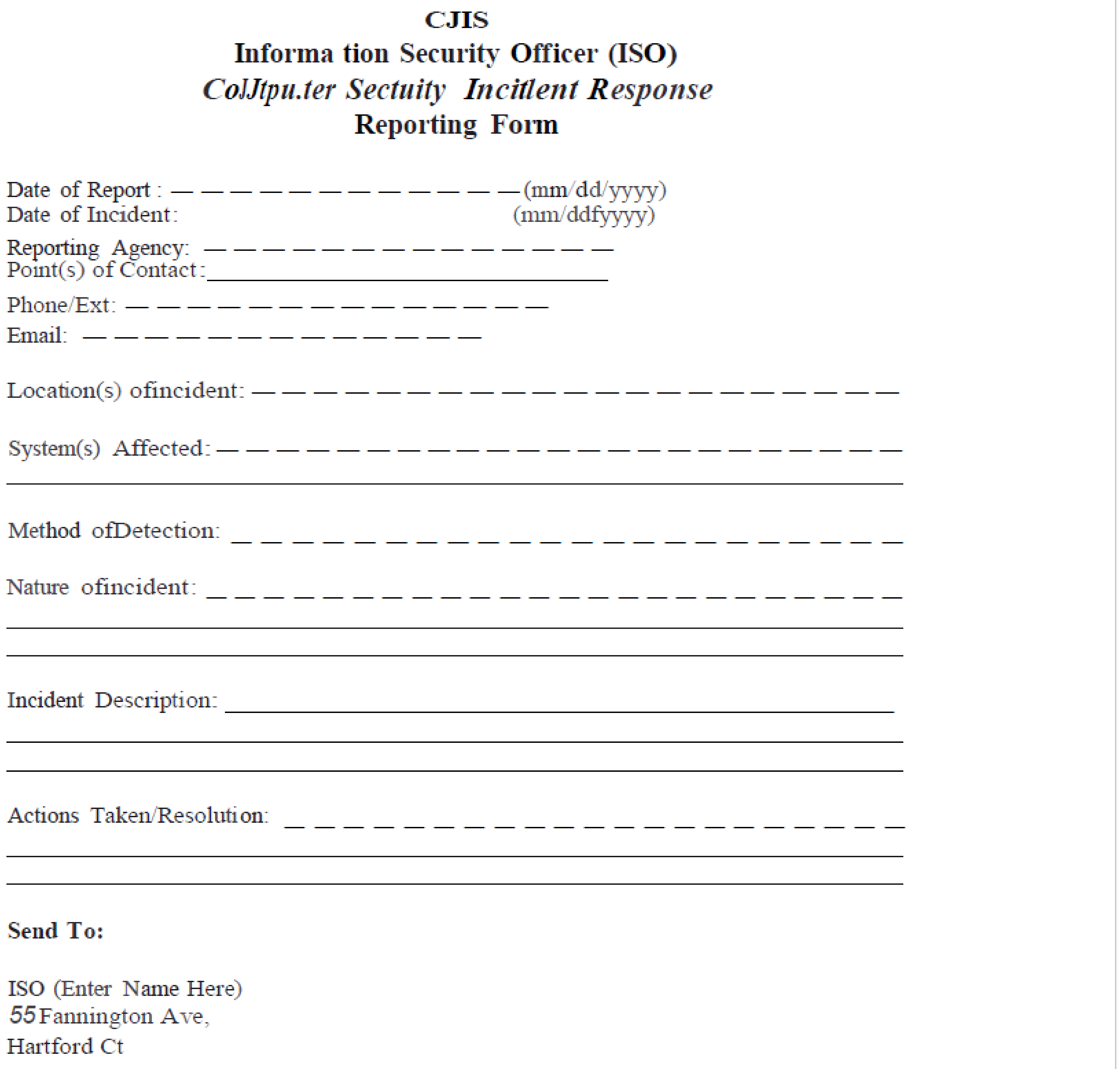
(Please reach out to CJIS-CT ISO for the sample Agreements/MOUs)

10. APPENDIX E: Online Security Forums and Organizations

i. FBI Criminal Justice Information Services Division (CJIS)
ii. Forrester Security Forum
iii. Forum of Incident Response and Security Teams (FIRST)
iv. International Organization for Standardization (ISO)
v. International Information Systems Security Certification Consortium, Inc. (ISC)
vi. Microsoft Developer Network (MSDN) Information Security
vii. National Institute of Standards and Technology (NIST)
viii. Open Web Application Security Project (OWASP)
ix. SANS (SysAdmin, Audit, Network, Security) Institute
x. Security Focus
xi. The Register
xii. US Computer Emergency Response Team (CERT)
xiii. US DoJ Computer Crime and Intellectual Property Section (CCIPS)

11. APPENDIX F: Sample forms

1. Security Incident Notification Report



CJIS
Informa tion Security Officer (ISO)
CoJJtpu.ter Sectuity Incitlent Response
Reporting Form

Date of Report : — — — — — — — — — — — — — (mm/dd/yyyy)
Date of Incident: (mm/ddfyyyy)

Reporting Agency: — — — — — — — — — — — — — — —
Point(s) of Contact:____________________________

Phone/Ext: — — — — — — — — — — — — — — —

Email: — — — — — — — — — — — — — —

Location(s) ofincident: —

System(s) Affected: —

Method ofDetection: _

Nature ofincident: _

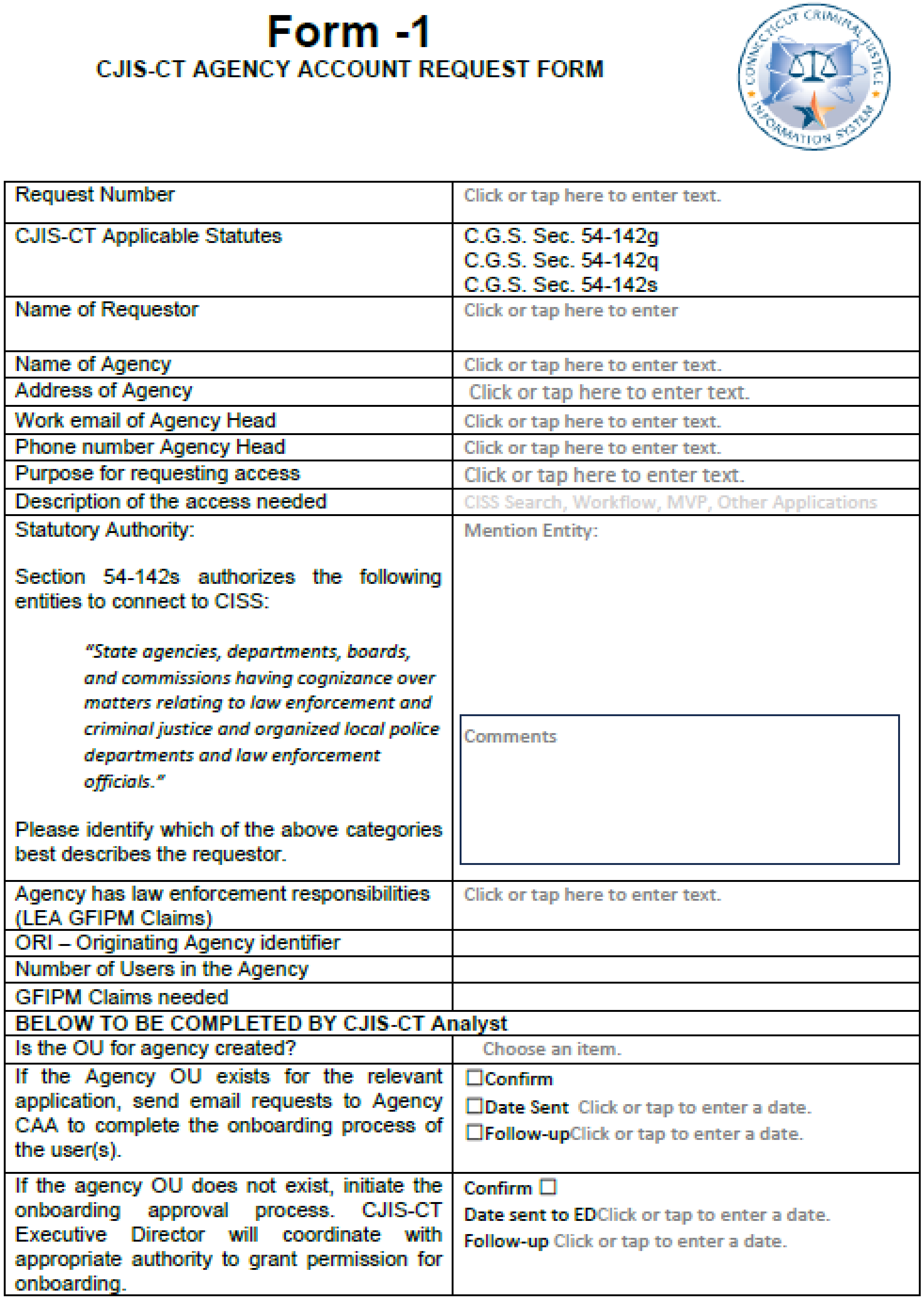
Incident Description: ______________________________________

Actions Taken/Resolution: _

Send To:

ISO (Enter Name Here)
55 Fannington Ave,
Hartford Ct

2. Form 1



Form -1

CJIS-CT AGENCY ACCOUNT REQUEST FORM

Request Number	Click or tap here to enter text.
CJIS-CT Applicable Statutes	C.G.S. Sec. 54-142g C.G.S. Sec. 54-142q C.G.S. Sec. 54-142s
Name of Requestor	Click or tap here to enter
Name of Agency	Click or tap here to enter text.
Address of Agency	Click or tap here to enter text.
Work email of Agency Head	Click or tap here to enter text.
Phone number Agency Head	Click or tap here to enter text.
Purpose for requesting access	Click or tap here to enter text.
Description of the access needed	CISS Search, Workflow, MVP, Other Applications
Statutory Authority: Section 54-142s authorizes the following entities to connect to CISS: *"State agencies, departments, boards, and commissions having cognizance over matters relating to law enforcement and criminal justice and organized local police departments and law enforcement officials."* Please identify which of the above categories best describes the requestor.	Mention Entity: Comments
Agency has law enforcement responsibilities (LEA GFIPM Claims)	Click or tap here to enter text.
ORI – Originating Agency identifier	
Number of Users in the Agency	
GFIPM Claims needed	
BELOW TO BE COMPLETED BY CJIS-CT Analyst	
Is the OU for agency created?	Choose an item.
If the Agency OU exists for the relevant application, send email requests to Agency CAA to complete the onboarding process of the user(s).	☐**Confirm** ☐**Date Sent** Click or tap to enter a date. ☐**Follow-up**Click or tap to enter a date.
If the agency OU does not exist, initiate the onboarding approval process. CJIS-CT Executive Director will coordinate with appropriate authority to grant permission for onboarding.	**Confirm** ☐ **Date sent to ED**Click or tap to enter a date. **Follow-up** Click or tap to enter a date.

Form -1

CJIS-CT AGENCY ACCOUNT REQUEST FORM

APPROVED BY

--- ----------------------------------

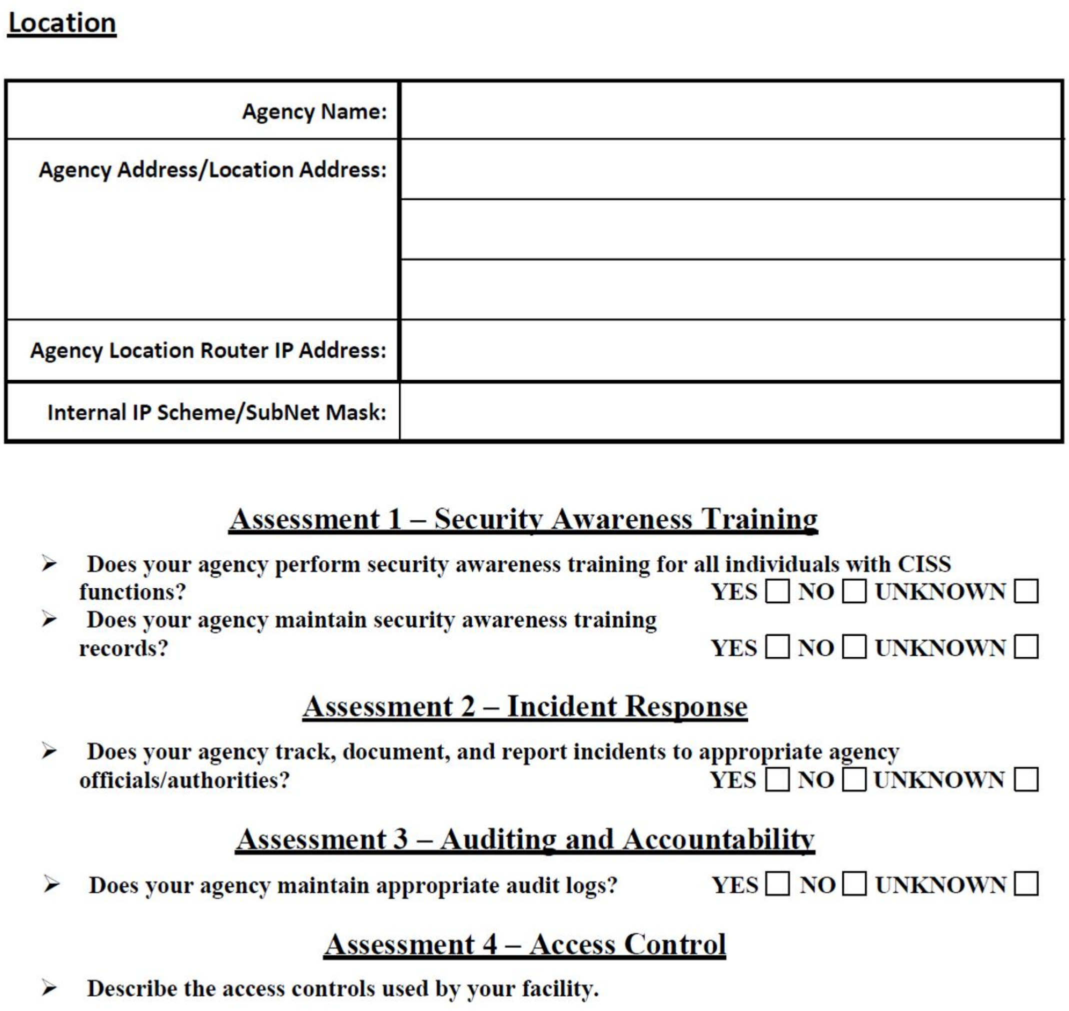
Requestor Agency Head/Designee DATE

--- ----------------------------------

CJIS-CT Executive Director DATE

Please reach out to cjis.helpdesk@ct.gov for any support.
CUAR Form 1, February 19, 2025

CJIS-CT Security Compliance Assessment Form (CJIS-2)



Location

Agency Name:	
Agency Address/Location Address:	
Agency Location Router IP Address:	
Internal IP Scheme/SubNet Mask:	

Assessment 1 – Security Awareness Training

- **Does your agency perform security awareness training for all individuals with CISS functions?** **YES □ NO □ UNKNOWN □**
- **Does your agency maintain security awareness training records?** **YES □ NO □ UNKNOWN □**

Assessment 2 – Incident Response

- **Does your agency track, document, and report incidents to appropriate agency officials/authorities?** **YES □ NO □ UNKNOWN □**

Assessment 3 – Auditing and Accountability

- **Does your agency maintain appropriate audit logs?** **YES □ NO □ UNKNOWN □**

Assessment 4 – Access Control

- **Describe the access controls used by your facility.**

Assessment 5 – Identification and Authentication

- Describe how you authenticate and identify your users.

Assessment 6 – Configuration Management

- Please submit a network topology diagram depicting your connectivity to CISS.

Assessment 7 – System and Information Integrity

Firewalls

- Is the CJIS portion of your agency's network segment protected by a firewall? YES □ NO □ UNKNOWN □
- Is this firewall configured to allow only permissible protocols and traffic inherent to your agency's network environment? YES □ NO □ UNKNOWN □
- Is this firewall configured to perform logging and audit capability? YES □ NO □ UNKNOWN □
- Is this firewall configured to retain logs for a minimum of one (1) year? YES □ NO □ UNKNOWN □

Workstations and Laptops

Hardware and Operating Systems

- How many total workstations and laptops are in your network environment? Please list operating systems used and count of operating systems:

Operating System	Version	Number
Windows	7	
Other		
Other		
Other		

- **Is each of the above devices and its operating system presently under contract for maintenance and support with its manufacturer? YES □ NO □ UNKNOWN □**
- **Have you performed "OS Hardening" on each of the above devices to reduce vulnerabilities in the computer hardware and operating system? YES □ NO □ UNKNOWN □**
- **Do you practice least privilege on each of the above devices to reduce vulnerabilities in the computer hardware and operating system? YES □ NO □ UNKNOWN □**

Anti-Virus Program

- **Are all workstations and laptops residing within your agency accessing CISS protected by a currently supported virus protection program? YES □ NO □ UNKNOWN □**
- **Does the Anti-Virus program on each workstation and laptop receive virus signature updates automatically? YES □ NO □ UNKNOWN □**
  - **If NO, please explain any existing process**

Patch Management Process

- **Are all workstations and laptops residing within your agency accessing CISS protected by a patch management program? YES □ NO □ UNKNOWN □**
- **Does the patch management application receive updates automatically? YES □ NO □ UNKNOWN □**
  - **If NO, please explain any existing process**

- **Are these patches applied to each workstation and laptop through an automated process? YES □ NO □ UNKNOWN □**
  - **If NO, please explain any existing process**

Browsers

- **How many total workstations and laptops are browser-enabled?**
- **How many utilize each of the following browsers?**

Browser	Version	Number
Internet Explorer	8	
Other		
Other		
Other		

Servers

Hardware and Operating Systems

- **How many total servers are in your network environment?**
- **Please list operating systems used and count of operating systems:**

Operating System	Version	Number
Windows	7	
Other		
Other		
Other		

- **Is each of the above servers and its operating system presently under contract for maintenance and support with its manufacturer? YES □ NO □ UNKNOWN □**
- **Have you performed "OS Hardening" on each of the above servers to reduce vulnerabilities in the computer hardware and operating system? YES □ NO □ UNKNOWN □**

Anti-Virus Program

- **Are all servers residing within your agency accessing CISS protected by a currently supported virus protection program? YES □ NO □ UNKNOWN □**

- ➢ **Does the Anti-Virus program on each server receive virus signature updates automatically?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain any existing process**

____

____

____

____

Patch Management Process

- ➢ **Are all servers residing within your agency accessing CISS protected by a patch management program?** **YES □ NO □ UNKNOWN □**
- ➢ **Does the patch management application receive updates automatically?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain any existing process**

____

____

____

____

- ➢ **Are these patches applied to each server through an automated process?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain any existing process**

____

____

____

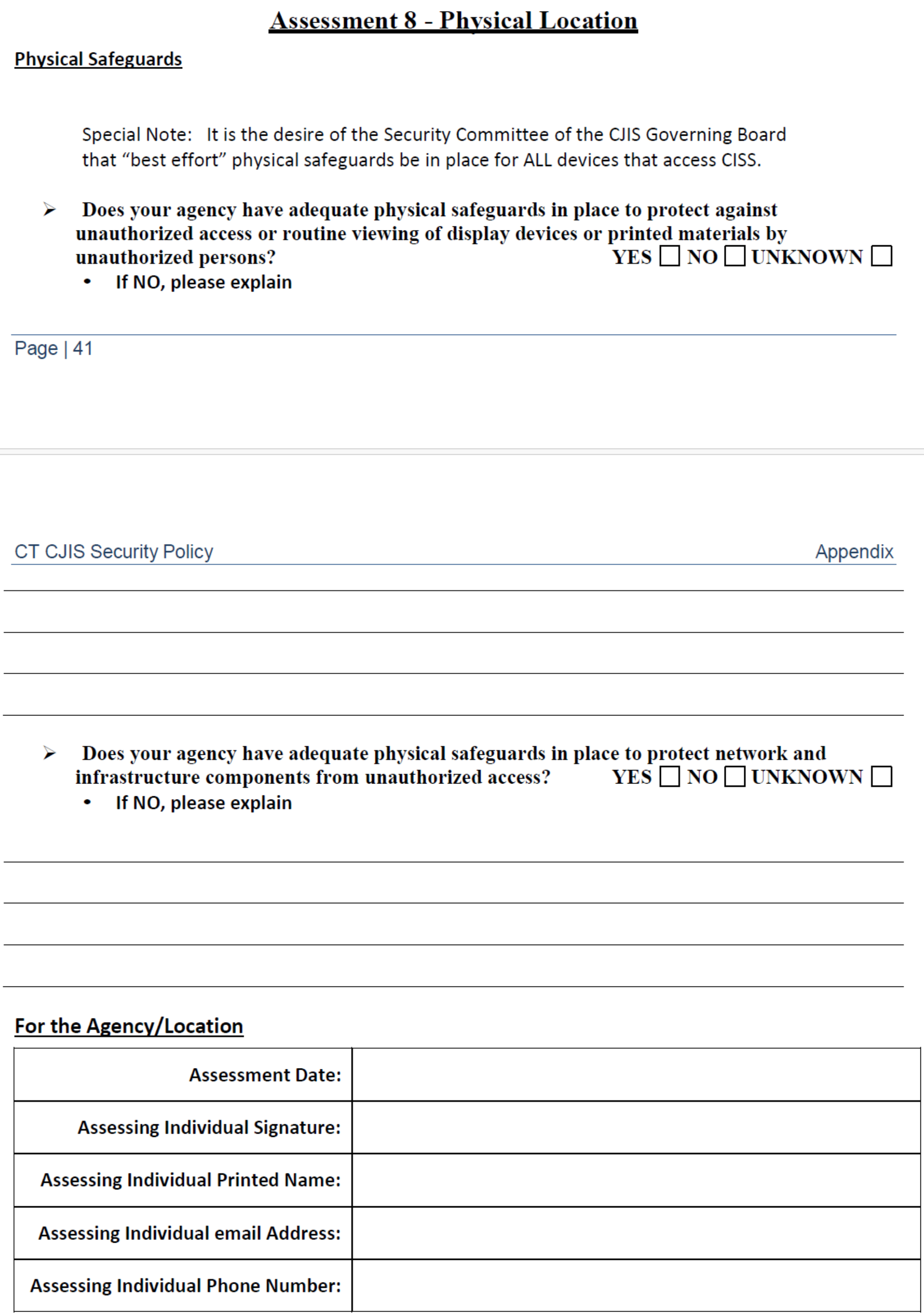
____

Assessment 8 - Physical Location

Physical Safeguards

Special Note: It is the desire of the Security Committee of the CJIS Governing Board that "best effort" physical safeguards be in place for ALL devices that access CISS.

- ➢ **Does your agency have adequate physical safeguards in place to protect against unauthorized access or routine viewing of display devices or printed materials by unauthorized persons?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain**



Assessment 8 - Physical Location

Physical Safeguards

Special Note: It is the desire of the Security Committee of the CJIS Governing Board that "best effort" physical safeguards be in place for ALL devices that access CISS.

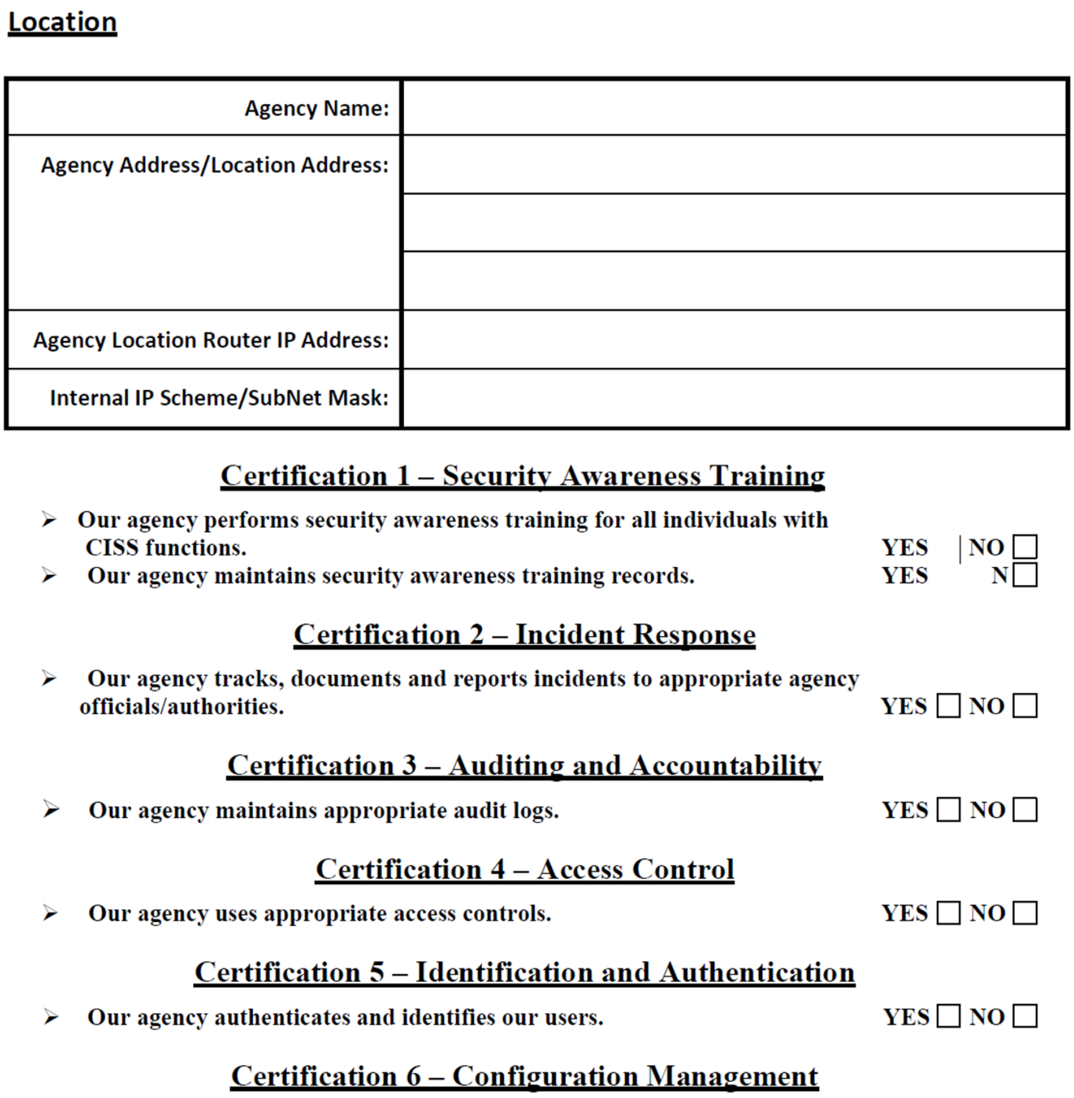
- **Does your agency have adequate physical safeguards in place to protect against unauthorized access or routine viewing of display devices or printed materials by unauthorized persons?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain**

- **Does your agency have adequate physical safeguards in place to protect network and infrastructure components from unauthorized access?** **YES □ NO □ UNKNOWN □**
  - **If NO, please explain**

For the Agency/Location

Assessment Date:	
Assessing Individual Signature:	
Assessing Individual Printed Name:	
Assessing Individual email Address:	
Assessing Individual Phone Number:	

FORM 3 – CJIS-CT Security Compliance Certification Form (CJIS-3)



Location

Agency Name:	
Agency Address/Location Address:	
Agency Location Router IP Address:	
Internal IP Scheme/SubNet Mask:	

Certification 1 – Security Awareness Training

- ➢ **Our agency performs security awareness training for all individuals with CISS functions.** **YES | NO □**
- ➢ **Our agency maintains security awareness training records.** **YES N□**

Certification 2 – Incident Response

- ➢ **Our agency tracks, documents and reports incidents to appropriate agency officials/authorities.** **YES □ NO □**

Certification 3 – Auditing and Accountability

- ➢ **Our agency maintains appropriate audit logs.** **YES □ NO □**

Certification 4 – Access Control

- ➢ **Our agency uses appropriate access controls.** **YES □ NO □**

Certification 5 – Identification and Authentication

- ➢ **Our agency authenticates and identifies our users.** **YES □ NO □**

Certification 6 – Configuration Management

- **We have submitted a network topology diagram depicting our connectivity to CISS.** **YES □ NO□**

Certification 7 –System and Information Integrity

Firewalls

- **The CJIS portion of our agency's network segment is protected by a firewall.** **YES NO □**
- **This firewall is configured to allow only permissible protocols and traffic inherent to our agency's network environment.** **YES NO □**
- **This firewall is configured to perform logging and audit capability.** **YES N□**
- **This firewall is configured to retain logs for a minimum of one (1) year.** **YES N□**

Workstations and Laptops

Hardware and Operating Systems

- **All workstations and laptops residing within our agency that access CISS utilize an operating system presently supported by its manufacturer.** **YES □ NO □**
- **All workstations and laptops residing within our agency that access CISS have been "OS hardened" to reduce vulnerabilities and mitigate potential risks.** **YES □ NO □**

Anti-Virus Program

- **All workstations and laptops residing within our agency that access CISS are protected by a currently supported virus protection program.** **YES □ NO □**
- **There is a process in place for these workstations and laptops to receive virus patterns in an automated fashion.** **YES □ NO □**

Patch Management Process

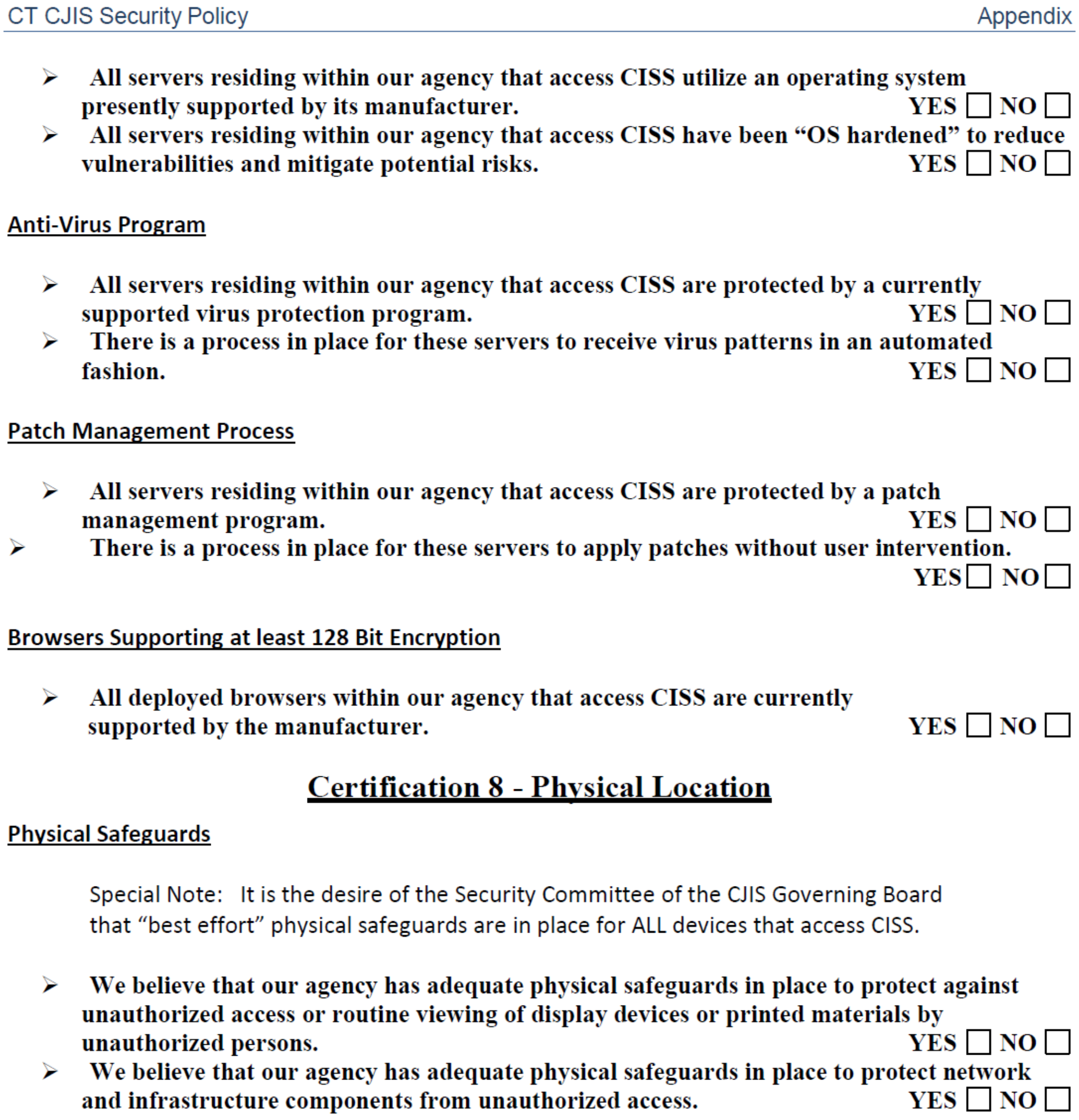
- **All workstations and laptops residing within our agency that access CISS are protected by a patch management program.** **YES □ NO □**
- **There is a process in place for these workstations and laptops to apply patches without user intervention.** **YES □ NO □**

Browsers Supporting at least 128 Bit Encryption

- **All deployed browsers within our agency that access CISS are currently supported by the manufacturer.** **YES □ NO □**

Servers

Hardware and Operating Systems



- **All servers residing within our agency that access CISS utilize an operating system presently supported by its manufacturer.** **YES □ NO □**
- **All servers residing within our agency that access CISS have been "OS hardened" to reduce vulnerabilities and mitigate potential risks.** **YES □ NO □**

Anti-Virus Program

- **All servers residing within our agency that access CISS are protected by a currently supported virus protection program.** **YES □ NO □**
- **There is a process in place for these servers to receive virus patterns in an automated fashion.** **YES □ NO □**

Patch Management Process

- **All servers residing within our agency that access CISS are protected by a patch management program.** **YES □ NO □**
- **There is a process in place for these servers to apply patches without user intervention.** **YES□ NO □**

Browsers Supporting at least 128 Bit Encryption

- **All deployed browsers within our agency that access CISS are currently supported by the manufacturer.** **YES □ NO □**

Certification 8 - Physical Location

Physical Safeguards

Special Note: It is the desire of the Security Committee of the CJIS Governing Board that "best effort" physical safeguards are in place for ALL devices that access CISS.

- **We believe that our agency has adequate physical safeguards in place to protect against unauthorized access or routine viewing of display devices or printed materials by unauthorized persons.** **YES □ NO □**
- **We believe that our agency has adequate physical safeguards in place to protect network and infrastructure components from unauthorized access.** **YES □ NO □**

Certification 9 - General

- **Our agency understands that noncompliance of any of these certifications may result in sanctions, as adopted by the CJIS Governing Board, being levied on our agency which may result in, but are not limited to, the removal of access rights to CISS. YES □ NO □**
- **Our agency understands that our location may be subject to an audit by representative(s) of the CJIS Security Committee. YES □ NO □**
- **Our agency understands that any additional devices that connect to CISS after the approval of this form must also comply with these certifications and are subject to the same policies. YES □ NO □**
- **Our agency understands that, upon return receipt of this form signed and approved by the CJIS Support Group, this agency is granted permission to access CISS from any compliant device effective the date of the approving signature. YES □ NO □**

I HEREBY CERTIFY THAT, TO THE BEST OF MY KNOWLEDGE AND BELIEF, THE INFORMATION CONTAINED HEREIN IS TRUE AND CORRECT.

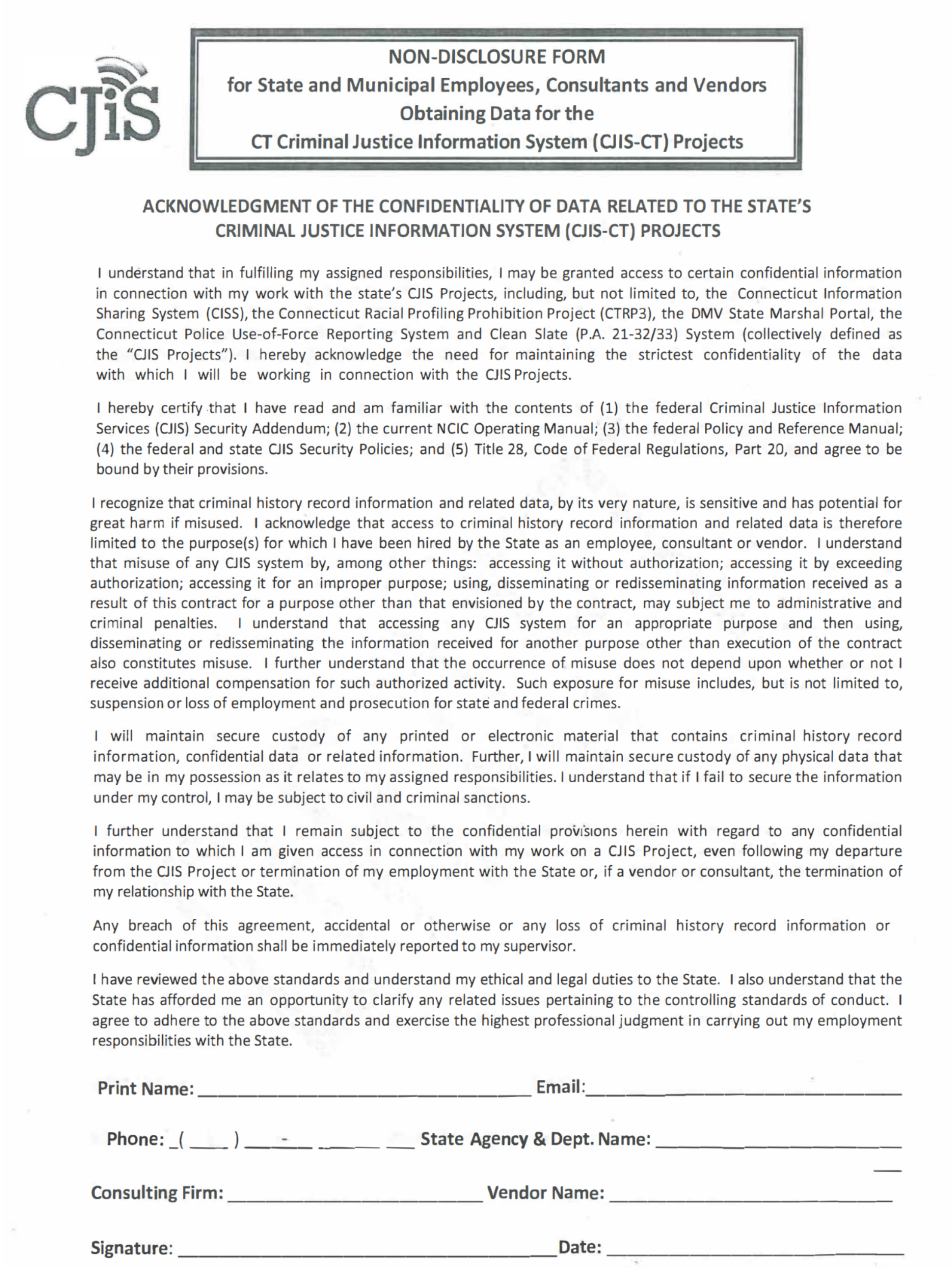
For the Agency

Certification Date:	
Certifying Individual Signature:	
Certifying Individual Printed Name:	
Certifying Individual email Address:	
Certifying Individual Phone Number:	
Agency Head Signature:	
Agency Head Printed Name:	

For the CJIS Support Group

Approval Date:	
Approving Individual Signature:	

Non-Disclosure Agreements



NON-DISCLOSURE FORM
for State and Municipal Employees, Consultants and Vendors Obtaining Data for the CT Criminal Justice Information System (CJIS-CT) Projects

ACKNOWLEDGMENT OF THE CONFIDENTIALITY OF DATA RELATED TO THE STATE'S CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS-CT) PROJECTS

I understand that in fulfilling my assigned responsibilities, I may be granted access to certain confidential information in connection with my work with the state's CJIS Projects, including, but not limited to, the Connecticut Information Sharing System (CISS), the Connecticut Racial Profiling Prohibition Project (CTRP3), the DMV State Marshal Portal, the Connecticut Police Use-of-Force Reporting System and Clean Slate (P.A. 21-32/33) System (collectively defined as the "CJIS Projects"). I hereby acknowledge the need for maintaining the strictest confidentiality of the data with which I will be working in connection with the CJIS Projects.

I hereby certify that I have read and am familiar with the contents of (1) the federal Criminal Justice Information Services (CJIS) Security Addendum; (2) the current NCIC Operating Manual; (3) the federal Policy and Reference Manual; (4) the federal and state CJIS Security Policies; and (5) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which I have been hired by the State as an employee, consultant or vendor. I understand that misuse of any CJIS system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or redisseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing any CJIS system for an appropriate purpose and then using, disseminating or redisseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

I will maintain secure custody of any printed or electronic material that contains criminal history record information, confidential data or related information. Further, I will maintain secure custody of any physical data that may be in my possession as it relates to my assigned responsibilities. I understand that if I fail to secure the information under my control, I may be subject to civil and criminal sanctions.

I further understand that I remain subject to the confidential provisions herein with regard to any confidential information to which I am given access in connection with my work on a CJIS Project, even following my departure from the CJIS Project or termination of my employment with the State or, if a vendor or consultant, the termination of my relationship with the State.

Any breach of this agreement, accidental or otherwise or any loss of criminal history record information or confidential information shall be immediately reported to my supervisor.

I have reviewed the above standards and understand my ethical and legal duties to the State. I also understand that the State has afforded me an opportunity to clarify any related issues pertaining to the controlling standards of conduct. I agree to adhere to the above standards and exercise the highest professional judgment in carrying out my employment responsibilities with the State.

Print Name: ________________________________ **Email:** ______________________________

Phone: _(____) ______- ______ ___ **State Agency & Dept. Name:** ________________________

Consulting Firm: _________________________ **Vendor Name:** ____________________________

Signature: ____________________________________ **Date:** ____________________________

12. APPENDIX G: Best Practices

(With reference to FBI Security Policy and NIST Standards)

12.1 G.1 Cloud Computing

Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- FBI Security Policy Version 6.0

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.
Cloud subscriber – A person or organization that is a customer of a cloud
Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber
Cloud provider – An organization that provides cloud services
CJIS Security Policy – Refers to the FBI CJIS Security Policy

Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The "cloud" spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

One of the benefits of cloud computing is the ability to outsource many of the technical functions agencies may not want to perform for various reasons. Ultimately, the move to cloud computing is a business and security risk decision in which the following relevant factors are given proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

Achieving CJIS Security Policy Compliance:

The question that is often asked is, "Can an Agency be compliant with the CJIS Security Policy and also cloud compute?"
Because the CJIS Security Policy is device and architecture independent, the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CJIS Security Policy.
There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.
Admittedly, the existing CJIS Security Policy requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren't new to vendors serving the criminal justice community and many vendors have been successfully meeting the Policy requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

General CJIS Security Policy Applicability Questions

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. Asking the following general questions will help frame the process of determining compliance with the existing requirements of the CJIS Security Policy.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access?

- Will advanced authentication (AA) be required for access to CJI within a cloud environment?

- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location?

- Are the encryption requirements being met?
    - Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? *Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI.*
    - Is the data encrypted while at rest and in transit?

- What are the cloud service provider's incident response procedures?
    - Will the cloud subscriber be notified of any incident?
    - If CJI is compromised, what are the notification and response procedures?

- Is the cloud service provider a private contractor/vendor?
    - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI?

- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits?

Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter housing and processing CJI.

- How will event and content logging be handled?
    - Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request?
    - What are the cloud service provider's responsibilities with regard to media protection and destruction?

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CJIS Security Policy, device and architecture independence permits the use of cloud computing, but the security requirements do not change.

Cloud Utilization Scenarios

1. Encrypted CJI in a Cloud Environment–Key Management Control, Security Awareness Training, and Personnel Controls

Prior to permitting CJI to be stored or traverse through a cloud environment, the agency should ensure proper encryption key management control procedures are implemented to determine who has access and control over the encryption keys. Proper key management control is vital to CJI security as those individuals (agency or cloud employees) with access to the keys can decrypt the stored files, and therefore, have unescorted access to unencrypted CJI. This means all those individuals must be subjected to security awareness training requirements as individuals with unescorted access to unencrypted CJI.

a. Scenario 1–Agency Stores CJI in a Cloud:

A CJA stores encrypted CJI (Backup files and drives) in a cloud service provider's environment. To access CJI, the agency will extract the CJI from the cloud to its local machine and then decrypt the CJI. The CJI is processed, re-encrypted, and then re-uploaded to the cloud environment for storage. In this scenario, the agency always encrypts the CJI prior to placing it in the cloud and only authorized users of the agency have access to the encryption keys. Since the agency maintains the encryption keys, the cloud service provider employees would not need to undergo fingerprint-based background checks, nor have security awareness training. These requirements are negated, because only authorized personnel with access to the keys have the ability to view this CJI in an unencrypted form.

b. Scenario 2–Agency Accesses CJI While in a Cloud:

A CJA stores CJI (files and drives) in a cloud service provider's environment, but as part of daily operations authorized users will remotely access the encrypted CJI in the cloud. The user will decrypt the CJI while it is in the cloud's virtual environment, process the data, and then re-encrypt the data prior to ending the remote session. The agency maintains the keys and the cloud service provider does not have access to the encryption keys. However, since the CJI is decrypted within the cloud's virtual environment, any administrative personnel employed by the cloud provider having the ability to access the virtual environment must be identified and subjected to security awareness training and personnel security controls as described in the CJIS Security Policy.

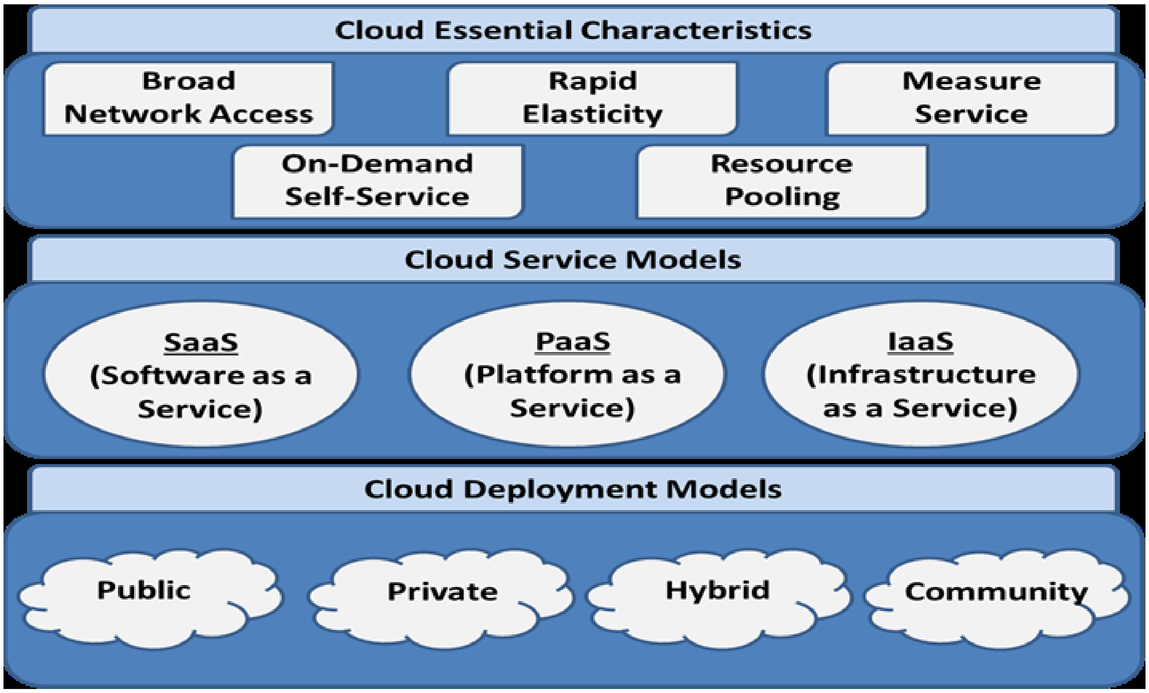
c. Scenario 3–CJI Impact from a Cloud Datacenter Critical Systems Crash–Core Dump* Recovery:

A CJA utilizes a cloud service provider (IaaS or PaaS) to store CJI and remotely accesses the environment to process CJI. During normal operation, the cloud provider experiences systems outages within the datacenter in which CJI is processed and stored. The cloud provider's administrators need to repair the systems and restore service using data from a core dump to return to normal operations. The cloud service provider as part of the Service Level Agreement (SLA) with the CJA has been authorized to maintain the encryption keys in order respond to such an event. The cloud administrators with such access have underwent fingerprint-based background checks and security awareness training. This allows the cloud administrators to decrypt CJI so that it is written to the core dump files for restoration following the system outage. CJI, however, is encrypted at all times except when part of the core dump files. As part of the SLA, the cloud service provider has agreed to treat the core dump files as CJI to ensure all protection are in place in compliance with the CJIS Security Policy.

* Core Dump - A file of a computer's documented memory of when a program or computer crashed. The file consists of the recorded status of the working memory at an explicit time, usually close to when the system crashed or when the program ended atypically as it presents the risk that the system failure would ensure the loss of the encrypted data.

The Cloud Model Explained:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown below.



Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

On-demand self-service
A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access
Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in which the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity
Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service
Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

** Typically this is done on a pay-per-use or charge-per-use basis.*

Deployment Models:

Private cloud
The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud
The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

Cloud providers offer different levels of service, i.e.; Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The way CJI is placed and accessed in the cloud determines if the personnel security requirements apply. Access to encryption keys and management of the resources vary depending on what type of service is used. The SaaS offering is the most likely service wherein the cloud service provider may have access to unencrypted CJI due to software updates, patches, and management. However, through management and control of encryption keys, all service offerings may be implemented in an agency-controlled manner where the cloud service provider has no ability to access unencrypted CJI.
For cloud computing services that involve the storage, processing, or transmission of CJI, security terms and requirements apply to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI. It is critical for the agency to understand the level of service and access required for each cloud implementation.

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure*.

** A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction* *layer sits above the physical layer.*

The SaaS service model is often referred to as “Software deployed as a hosted service and accessed over the Internet.”
The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.
When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider’s applications running on a cloud infrastructure*.

* A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

The SaaS service model is often referred to as “Software deployed as a hosted service and accessed over the Internet.”
The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.
When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Infrastructure as a Service (IaaS)
This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.
When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

Key Security and Privacy Issues:
Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service

models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—*at the extreme, displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

Governance

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Law and Regulations

Cloud providers are becoming more sensitive to legal and regulatory concerns and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea. When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Electronic Discovery

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Insider Access

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

Data Ownership

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Visibility

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

Ancillary Data
While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

Risk Management
Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture
The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

Identity and Access Management
Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

Software Isolation
High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

Data Protection
Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore,

must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

Value Concentration

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

Data Isolation

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools

resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Data Sanitization

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

Encryption

Client end-to-end encryption (e.g., encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.

- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.

- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

Data Availability

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

Incident Analysis and Resolution

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and

preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

General Recommendations:

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Security and Privacy Issue Areas and Recommendations

Areas	Recommendations
Governance	• Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services.
	• Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	• Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements.
	Compliance
	• Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements.
	• Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications
Trust	• Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time.
	• Establish clear, exclusive ownership rights over data.
	• Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system.
	• Continuously monitor the security state of the information system to support on-going risk management decisions.
Architecture	• Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	• Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	• Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	• Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.
	• Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value.

Areas	Recommendations
	• Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Availability	• Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements.
	• Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	• Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization.
	• Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.
	• Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

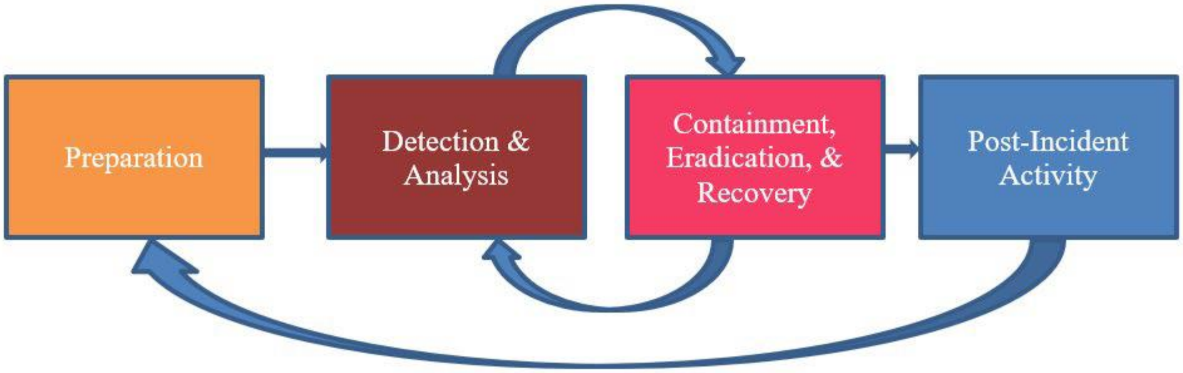
12.2 G.2 Incident Response

Information technology (IT) security incident response is an important and critical component of information technology programs. Performing incident response effectively can be a complex undertaking – for that reason, establishing a successful incident response capability requires planning and resources. Everyone in an organization must be aware of IT security risks, threats, and actions to take in situations where an actual IT security incident has occurred. Even the best-secured and controlled environments can experience these security risks, threats, events, and incidents. This document provides guidelines for appropriate response to IT security incidents, and are independent of specific hardware platforms, operating systems, protocols, or applications.

The following example incidents are used to highlight appropriate actions during each phase:

- Malicious code execution
- Ransomware execution
- Denial of service attack
- Social Engineering
- Phishing

NIST Special Publication 800-61 rev. 2 outlines the "Incident Response Life Cycle" as a collection of phases – distinct sets of activities that will assist in the handling of a computer security incident, from start to finish. The following diagram explains the process flow of the incident response life cycle:



Preparation

The initial phase of the incident response life cycle, "Preparation", involves establishing and training an incident response team, and acquiring the necessary tools and resources. A computer security incident may not have happened at this phase, but it is important to utilize all available knowledge and security measures to obtain the best posture for responding to potential future incidents. One of the most important preparation steps involves the collection, storage, and accessibility of event data and telemetry from hardware and software resources such as firewall logs, application logs, operating system logs, and other valuable sources of situational data, as well as the output of products that perform analysis on such data. Preventive measures to mitigate or eliminate future incidents are deployed during this phase, using industry best practices, data

obtained from research and intelligence sources, and lessons learned from past incidents.
It is also imperative to prepare a list of contact information or notification methodologies to employ when an incident occurs, as well as notification and communication strategies within the team, with stakeholders, and with upper management and potentially other criminal justice and non-criminal justice agencies. This will help ensure that when incidents arise, the proper personnel and organizations are notified and kept informed of the circumstances regarding the incident.
Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Preparation phase can be given:

Malicious code execution

Preparation for incidents involving malicious code execution should initially involve user awareness of sources of malicious code. There are many potential sources of malicious code, such as web pages, emails, and removable media. The utilization and deployment of effective antivirus software, integrity-monitoring software, and intrusion detection and prevention software are effective measures to take to prepare for incidents involving malicious code execution.

Ransomware execution

Preparation phase activities for incidents involving ransomware execution are much the same as activities for malicious code execution, as ransomware is a specialized form of malware that encrypts potentially important or critical files, with the intention of coercing a victim to pay for a decryption key. Implementing a robust offline backup solution for these types of files is an important preparative action to take regarding the execution of ransomware. This will ensure that when ransomware attacks do happen, the mission impact is as minimal as possible and very little or no data is lost.

Denial of service attack

Denial of service attacks are given attention in the preparation phase. Defensive responses to denial of service attacks typically involve the use of a combination of attack detection and traffic classification and response tools, aiming to block traffic identified as abusive denial of service activity. Deploying solutions such as IDS/IPS devices and software, network hardware with rate-limiting capabilities (routers, switches, and firewalls), and upstream filtering devices at the system perimeter can mitigate for denial of service attacks.
Social Engineering
Preparation for social engineering attacks starts with user awareness training. Understanding and identifying attempts to obtain information in an unauthorized manner is crucial to thwarting these types of scenarios. Social engineering is the art of manipulating people to obtain information they may not be authorized to handle. Training and routinely testing users on potential social engineering scenarios and tactics, and providing training regarding appropriate responses to requests involving personal or otherwise sensitive information (for example, passwords or criminal justice information), is an effective way to ensure social engineering attacks never traverse past the preparation phase of the incident response life cycle.

Phishing

Like social engineering, preparation for phishing attacks is imperative. Phishing is a social engineering technique attackers employ to deceive users, in a fraudulent attempt to obtain sensitive information, or to gain unauthorized access to systems. Phishing is extremely widespread, and attackers disguising fraudulent scenarios in electronic communication such as email and instant messages are the most common. User awareness of these types of tactics is paramount to prepare for phishing attacks and schemes.

Detection and Analysis

The detection and analysis phase begins when a security incident has occurred. To understand when this phase begins, there must be a capability for an intelligent determination of circumstances constituting a security incident. Specialized knowledge and highly trained personnel are necessary for this step to be effective. Many organizations employ teams of personnel who are specifically trained to handle the intricacies of the incident response life cycle. The determination of a security incident can arise from one or several circumstances simultaneously – for example:

- Trained personnel manually reviewing collected event data for evidence of compromise
- Software applications analyzing events, trends, and patterns of behavior
- The observation of suspicious or anomalous activity on a computer system

The goals of this phase are:

- To detect whether a security incident occurred
- To determine the vector (i.e., method) of attack
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident
- To obtain or create intelligence products regarding attack vectors and methodologies, especially when dealing with malicious code

Prioritization of incidents is also an important decision point in the incident response life cycle, as the circumstances regarding an incident can bring the situation to a critical level. There are three major impacts to consider when addressing priority of incidents:

- Functional Impact: the impact to business functionality
- Information Impact: the impact to confidentiality, integrity, and/or availability of criminal justice information
- Recoverability: the amount of time and resources that must be spent on recovering from an incident

Documentation regarding an incident should be thorough and applicable to the incident. This can be crucial in incidents that may lead to legal prosecution, as well as being invaluable to efficiently document, track, handle, manage, and resolve one or more incidents at the same time.
Using the example incident categories outlined earlier, some overview into appropriate actions and

activities for the Detection and Analysis phase are given:

Malicious code execution

Detection of malicious code execution is often a primary job of host-based antivirus software. Having a capable and up-to-date antivirus solution installed on a system can detect known malicious code, as well as detect potentially malicious behaviors. The delivery of malicious code to a system can be detected by network traffic analysis and protection tools and hardware. Additionally, some malicious code may produce network traffic that is indicative of successful execution, exploitation, and/or compromise of a system. Solutions such as intrusion detection/prevention systems, Security Information and Event Management (SIEM) tools, and file integrity monitoring software can provide the necessary level of fidelity to make a determination of malicious code execution.

Knowing if or when a system is infected is not always immediately evident. Security controls may have been bypassed or even disabled by the malicious code. However, systems infected by malicious code or software (i.e., malware) can exhibit several indicators. These indicators include, but are not limited to:

- Unexpected pop-up windows
- Slow start up and/or slow performance
- Suspicious hard drive activity including an unexpected lack of storage space
- Missing files
- Crashes and/or error messages
- Unexplained network activity
- Hijacked email

Analysis of malicious code can be performed in several ways. Static analysis of malicious code can be performed to determine the capabilities of the malicious code and generate actionable intelligence. Dynamic analysis of malicious code can be used to observe how the malicious code interacts with the system and what actions it performs and can often more rapidly determine the capabilities of malicious code. Both static and dynamic analysis can be performed manually, as well as in an automated fashion. Trained specialized personnel are crucial to the analysis of malicious code.

Ransomware execution

The detection of ransomware is identical to the detection of malicious code. Ransomware is specialized malicious code that encrypts potentially valuable files, generally with the intent to coerce a victim to pay a ransom for the possibility of the decryption of those files. Host-based antivirus solutions can also detect these threats, and network traffic analysis and protection tools and hardware can be used to prevent the successful execution of ransomware. SIEM tools and file integrity monitoring software can also detect the execution of ransomware.

Analysis of ransomware is identical to the analysis of malicious code, and the same intelligence can be determined in the same fashion as with the analysis of malicious code. The most obvious sign that ransomware has affected a system is the existence of encrypted files, the disappearance of certain types of files, and/or the presence of "ransom notes" on the system, which contain instructions for payment to obtain a decryption key, which may or may not be legitimate.

Denial of service attack

Denial of service (DoS) attacks are often detected at the perimeter of an organization but can also be detected within the organization as well. Often, from a user's perspective, the signs of a DoS attack appear to be network performance or administrative maintenance related issues such as slow or broken network connections or down websites. Additionally, an administrator may notice ping time outs, event logs overflowing or alerts from network monitoring systems as issues that may identify a DoS attack. Intrusion detection and prevention software and platforms can detect denial of service attacks, as well as some network monitoring hardware and appliances, such as web application filters, routers, firewalls, and switches. Devices targeted by denial of service attacks can also detect the attacks in some instances, if they have the capabilities to determine explicit attack activity versus normal network traffic.

Analysis of denial of service attacks include the determination of the source traffic, the protocols used to generate the traffic, the service(s) targeted by the attack, and the potential impacts of the attack. Network monitoring devices can often provide these types of data, with the exception of potential impacts of denial of service attacks on systems.

Social Engineering

Detection of social engineering attacks is primarily based on the situational awareness of the individual targeted by social engineering. Given that social engineering is a broad topic that can involve the manipulation and exploitation of people in control of an information system, user awareness of social engineering attempts is crucial. If the target has security awareness training in detecting attempts to gain information or access in an unapproved manner, social engineering is easier to detect.

Analysis of social engineering attacks will generally rely on the recollection abilities of or documentation taken by the targets of the attack. Social engineering may not occur on an information system and may be completely carried out in-person. If the target can recollect or produce documentation regarding the social engineering attempt, the motivation and desired access can potentially be determined. For successful social engineering attempts, recollection and documentation of the attempt is crucial to determining the level of unauthorized access that was obtained.

Phishing

Detection of phishing attacks generally will first occur at an organization's email point of presence. Some organizations still run their own email servers, and many have migrated to cloud solutions. Having an on-premise email server or server farm or cluster will require additional functionality to detect phishing attempts. For example, the header content of the email will need to be read, as well as the content inside the body of the email, to check for potentially malicious content and potentially falsified data that may indicate a phishing email. Many cloud email providers have built this capability into their email solutions, but it is still possible for users to receive phishing emails, as attacker tactics and capabilities evolve daily. The most effective detection of phishing comes from heightened situational awareness of potential attacks. Validating the source of the email can uncover potential phishing attempts.

Analysis of phishing attacks involves examination of email headers, as well as contents of the body of the email. The body of the email may contain malicious content, attachments, or links to suspicious or malicious content. Manual or automated analysis activities can be performed on the email content. Analysis of these elements should be performed by trained specialized personnel to generate intelligence and aid with the determination of indicators of compromise.

Containment, Eradication, and Recovery

Containment activities for computer security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. Often, this requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels can be invaluable to the implementation of containment activities. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

Eradication efforts for a computer security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Recovery efforts for incidents involve restoration of affected systems to normal operation. This may include actions like restoring systems from backups, rebuilding systems from an agency-approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

Compromised hosts are often attacked during these phases, as attackers try to regain their foothold on compromised systems or systems on the same network or others in the logical vicinity.

Malicious code execution

Containment activities for malicious code execution involve the logical or physical isolation of the host from the attacker's control and from any mission services or systems that would be impacted by the compromised host. This may include putting the host in a restricted VLAN, using firewalls to block traffic, disconnecting it from the network completely, shutting it down, or disabling functionality. Exercise caution as malicious code may have capabilities to take further actions on a host in case communications with a command and control server are severed. It is important to understand the capabilities of the malicious code before taking containment actions.

Eradication activities include the removal of malicious code from the system. This may be as simple as removing files, configuration rules, accounts, and other persistent items that the malicious code utilizes to function and maintain a presence on the system. This phase also involves the discovery and removal of indicators of compromise on other systems, if applicable. It is imperative to remediate vulnerabilities that may have been exploited during eradication as well.

Recovery from malicious code execution generally is similar across many environments. Rebuilding the system from a clean baseline or restoring files from backup are typical activities that help restore the functionality of the system to continue the mission. Changing system passwords, installing patches, implementing tighter network access control, and ensuring appropriate levels of logging fidelity of the information system are integral parts of the recovery process

Ransomware execution

Containment for ransomware execution should be as swift and immediate as possible, as ransomware can execute and spread to accessible media at a rapid pace. Considering files are being encrypted or have already been encrypted, immediate action should be taken to logically or physically isolate the system by disconnecting network connectivity. It is up to the system owner whether to take the risk in powering off the system, as valuable forensic artifacts may be destroyed in the process, but it will halt the execution of the ransomware and protect potentially valuable files. Please note that containment of active ransomware execution is one of the only circumstances where measures such as immediate shutdown are recommended.

Eradication of ransomware does not need to occur in most circumstances, as the entire goal of ransomware is to encrypt files and leave "recovery" instructions to extort victims. The vast majority of ransomware will delete once encryption of files is complete, but it is possible that some ransomware is persistent and can remain on the system. If this is the case, analysis should be performed on the ransomware to determine its capabilities, and eradication activities will proceed in an identical fashion to malicious code execution eradication activities.

Recovery from ransomware execution involves restoring encrypted files from backup and may involve the rebuilding of an entire system depending on the extent of the encryption from the ransomware. If a robust offline backup solution for hosts is not present or not utilized on a regular basis, the loss of potentially valuable data may be incredibly costly in several areas to repair, to include man-hours, revenue, and business products, data, and intelligence.

Denial of service attack

Containment of denial of service attacks involve the modification of access control where the attack is occurring. For example, if a web or application server is experiencing a denial of service attack, the system itself, as well as network monitoring devices, should be examined to determine the source of the attack traffic. Once the source of the traffic is identified, modifications to access controls or rate-limiting features such as firewall access controls lists (ACLs) and web application filters can be employed to block the traffic. Care must be taken to determine if the observed traffic is actually intentionally malicious denial of service traffic, versus heavy legitimate network traffic. Implementing access control mechanisms or rate-limiting features may negatively affect the mission of the system. It is also important to note that manual containment in this fashion may not be entirely effective, as attackers can circumvent the ACL by changing the attacking IP address, protocol, or other attribute of the connection.

Eradication is not necessarily applicable in denial of service scenarios, unless a vulnerability or misconfiguration is being exploited to cause the denial of service condition. If this is the case, take steps to remediate the vulnerability or misconfiguration.

Recovery actions depend on the available resources of the information system. For example, on-premise load balancers can be used to distribute the traffic, whether legitimate or malicious, to other less-burdened systems. Many cloud providers and content delivery networks also have denial of service mitigation capabilities. It may also be prudent to increase the resources (memory, processing capacity) of internet-facing systems so that they can handle larger amounts of traffic simultaneously.

Social Engineering

Containment regarding social engineering attacks is dependent upon the information or access that was provided to the attacker. For example, if an attacker gained access to an account on a system following a social engineering attempt, the account should be administratively disabled and all sources of event data regarding that account should be immediately collected. If sensitive data was divulged to the attacker, the impact of the exposure of that data should be examined and mitigating activity should be initiated to determine or reduce the damage of the spread of the information.

Eradication regarding social engineering attacks also depends on the information or access provided to the attacker. Removing or limiting the provided access is a pertinent eradication action. If the information provided is a credential to a system, disable and remove the credential from the system. Eradication may also involve the physical detainment or removal of personnel from a site. Recovery actions for social engineering attacks are dependent on the information or access provided to the attacker. Additionally, security awareness training is an appropriate recovery action to ensure staff understands the threats of social engineering.

Phishing

Containment of phishing activity is tied very closely to the identification and analysis of the phishing activity. Understanding the tactics of the phishing attacker is paramount to deploying containment activities. Activities include, but are not limited to, administratively blocking sender email addresses and IPs, blocking potential malicious content in email via a web proxy, communicating with potential recipients, and implementation of email content or hyperlink blacklisting if possible. Phishing attacks can also include attempts to have users execute malicious code on systems, where containment activities regarding malicious code will be applicable.

Eradication of phishing attacks include the administrative removal of the emails from email systems, as well as eradication actions for malicious code if applicable.

Recovery from phishing attacks can include:

- Implementation and enforcement of the Domain Keys Identified Mail (DKIM) email authentication method, which can mitigate the possibility that attackers can send spoofed email
- Implementation and enforcement of Sender Policy Framework (SPF) to control and stop sender forgeries
- Implementation and enforcement of Domain-based Message Authentication, Reporting, and Conformance (DMARC), which enables message senders to indicate that their messages are protected with SPF and/or DKIM

Additionally, if malicious code is present in the phishing attack, recovery actions regarding malicious code may be applicable.

Post-Incident Activity

Post-incident activities occur after the detection, analysis, containment, eradication, and recovery from a computer security incident. Arguably one of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Some of the important items to consider:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Smaller incidents, and those that are similar to others that have been well documented, do not necessarily need much focus in this phase of incident response. Larger and less-understood security incidents should be the focus of a comprehensive post-mortem evaluation that outlines many of the items listed above and should include personnel that can have a direct impact on or are directly affected or responsible for the involved systems.

Post-incident activities such as these also help to serve as training opportunities for all parties involved in the incident, from victims to system administration personnel, to incident responders.

Malicious code execution

Post-incident activities for malicious code execution generally will follow similar patterns. A timeline of activity should have been prepared using digital forensic data collected during the detection and analysis phases of the incident. This timeline should include all affected systems and times of all activities and actions taken during the incident. Steps that victims and system administrators may have taken during the course of the incident, as well as in close proximity to the time range of the incident, are valuable items to document and discuss. Any deviation from organizational policy should be noted and taken as training items or assigned consequences in accordance with organizational policies. It may also be pertinent to ensure that appropriate information and intelligence sharing was performed during and after the incident occurred. Corrective actions that may have prevented the execution of malicious code, such as antivirus solutions, restrictions on where executables can run, tightened permissions, and script blockers for browsers, should be considered as a mitigation for the risks posed by malicious code threats. Web proxy blocks from information discovered during analysis can be utilized to ensure that malicious hosts are not contacted.

Ransomware execution

Post-incident activities for ransomware execution include all the activities involved with malicious code execution, with the addition of ensuring the functionality of a robust offline backup solution. An offline backup solution ensures that backup data is kept inaccessible to ransomware threats and is available if ransomware is successfully executed. A functional and frequent (such as daily incremental and weekly full) backup process helps ensure that business continuity is maintained in the event of issues and incidents.

Denial of service attack

Denial of service post-incident activities should include a timeline of traffic activities, as well as organizational responses to the attack traffic as well as the timeline of any business impacts and the damage associated with the impacts. Any attack precursors should be investigated and noted, and intelligence implemented to notify personnel and potentially take action as soon as attack traffic is observed. Impacts on affected systems should be noted, and a consensus should be reached on whether the systems should be upgraded or supplemented with load-balancing capabilities.

Social Engineering

Post-incident activities for social engineering incidents should include a timeline that includes all applicable activities, such as points of contact, narratives from the parties involved, CCTV footage (if applicable), system and network log files, and physical access control logging data. If unauthorized access was obtained, the impact of the access should be assessed and mitigating factors should be identified for inclusion to reduce the risk of future incidents (such as multifactor authentication, physical locks, greater CCTV coverage, improved physical access control, etc.). Security awareness training should be imperative if policy was breached, and information or access was given to unauthorized parties.

Phishing

Phishing post-incident activities should also include a timeline of actions taken since the phishing email was received, to include descriptions of the type of phishing campaign observed (malicious code, financial exploitation, credential harvesting, etc.), malicious attachments contained (if any), malicious or suspicious links in the body of emails, as well as narratives from recipients of the email and any potential victims, either self-reported or discovered through email, network, or host-based monitoring. If malicious code was included in the campaign, typical post-incident activities involving malicious code should be considered as well. Training opportunities can often arise from phishing attacks, whether successful or not, that can be valuable in giving employees better situational awareness regarding phishing.

The CJIS-CT Security Policy requires each agency with access to CJI to establish operational incident handling procedures (i.e., a local policy). Gleaning from the requirements in Section 5.9 Incident Response, the local policy may include the following elements:

- Overall incident handling procedures. This section describes and identifies the processes used locally how the agency successfully prepares for, manages, and recovers from an incident. It includes sections on:
    - Preparation
    - Detection and Analysis
    - Containment
    - Recovery
    - User response activities

- How the agency performs incident reporting. This section describes the process of notifying internal and external partners when an incident has occurred and how the incident is documented. It includes sections on: o Internal and external points of contact
    - Required tracking and reporting documents
    - Escalation procedures

- • Incident management procedures. This section describes the agency's approach to a consistent and repeatable approach to managing incidents. It includes sections on: o Roles and responsibilities

    - Incident-related information collection
    - Updating policies with lessons learned
    - Collection of evidence
    - Incident response training
    - Document and artifact retention

12.3 G.3 Business Continuity Management

Purpose

The purpose of this section is to define the best practices for ensuring the continuity of critical business operations in the face of disruptions, disasters, or crises. This aligns with the CJIS-CT commitment to resilience, risk mitigation, and rapid recovery.

Scope

This section applies to all departments, business units, and third-party service providers that support mission-critical operations.

Governance and Planning

- Establish a Business Continuity Management (BCM) framework aligned with FBI CJIS Security Policy Section Contingency Planning and ISO 22301.
- Assign roles and responsibilities to a Business Continuity Management Team (BCMT).
- Develop and maintain a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).
- Conduct a Business Impact Analysis (BIA) annually or after significant organizational changes.

Risk Assessment

- Identify and assess potential risks to critical operations, including natural disasters, cyberattacks, and supply chain disruptions.
- Integrate risk assessments with the CJIS-CT overall risk management framework.

Recovery Strategies

- Define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for all critical systems.
- Establish alternate work sites or remote access strategies.
- Ensure backup systems and redundant infrastructure are in place and tested regularly.

Testing and Exercising

- Conduct BCP/DRP testing at least semi-annually.
- Include table-top exercises, full-scale simulations, and unannounced drills.
- Document and remediate any gaps identified during testing.

Communication and Awareness

- Maintain an up-to-date Crisis Communication Plan.
- Train employees on their roles in business continuity and incident response.
- Ensure emergency contact information is accurate and accessible.

Review and Continuous Improvement

- Review the BCP and DRP annually or after significant changes.
- Implement lessons learned from incidents, exercises, and audits.
- Monitor regulatory and compliance changes impacting continuity planning.

Business Continuity Metrics (Suggested and will vary for each application)

Metric	Description	Frequency	Target / Threshold
RTO (Recovery Time Objective)	Maximum allowable downtime for a system or process	CISS Application	As defined by BIA
RPO (Recovery Point Objective)	Maximum data loss tolerance (time-based)	CISS Application	As defined by BIA
BCP/DRP Test Completion Rate	Percentage of planned BCP/DRP tests completed on schedule	Quarterly	≥ 95%
Time to Restore Critical Operations	Time taken to restore mission-critical operations during an actual incident	Post-incident	≤ Defined RTO
Staff Training Completion Rate	Percentage of employees trained on BCP annually	Annually	≥ 90%
Alternate Site Readiness	Availability and readiness status of alternate site	Bi-annually	100% operational readiness
Data Backup Success Rate	Percentage of successful backups for critical systems	Daily/Weekly	≥ 99%
Incident Recovery Audit Score	Results from post-incident audit or after-action review	Post-incident	≥ 80% compliance
Communications Drill Success Rate	Completion and effectiveness of emergency communication tests	Quarterly	≥ 95%
Business Impact Analysis Update Rate	Frequency of updating BIA based on operational or environmental changes	Annually or as needed	100% of affected areas

12.4 G.4 Identity and Access Management (IAM)

This appendix provides advanced best practices for implementing robust Identity and Access Management (IAM) in CJIS-compliant environments. It aligns with CJIS-CT Security Policy Sections 5.2 (Access Control) and 5.8 (Identification and Authentication) and incorporates modern technologies and methodologies to enhance security, accountability, and compliance.

1. Identity Lifecycle Management

i. Automate user provisioning, role assignment, and deprovisioning using centralized identity platforms.
ii. Integrate with authoritative identity sources (e.g., Active Directory, Azure AD, Okta Universal Directory).
iii. Maintain detailed audit logs of identity creation, changes, and access history.
iv. Implement periodic access reviews and certification campaigns for critical roles.

2. Identity Proofing and Personally identifiable information (PII) Protection

i. Conduct strong identity proofing during onboarding, verifying users through:

- Government-issued identification
- Biometric verification
- Background checks for sensitive roles

ii. Collect only the minimum necessary PII, in accordance with data minimization principles.
iii. Store Personally identifiable information (PII) using:

- AES-256 encryption at rest
- TLS 1.2+ encryption in transit
- Secure, access-controlled databases

iv. Apply data retention policies that enforce timely deletion or anonymization of PII no longer required.
v. Ensure compliance with relevant privacy laws and regulations.

3. Authentication: Multi-factor and Adaptive Multi-factor authentication

i. Enforce Multi-Factor Authentication (MFA) for all users accessing CJI, using:

- FIPS 140-2 compliant hardware tokens
- Time-based one-time passwords (TOTP)
- Biometric identifiers (facial/fingerprint recognition)
- Smartcards or PKI certificates

ii. Implement Adaptive MFA that dynamically adjusts security controls based on:

- Risk level (device health, geolocation, IP reputation)

- User behavior
- Time-of-day patterns

4. Role-Based Access and Least Privilege

i. Enforce Role-Based Access Control (RBAC) aligned with job responsibilities.
ii. Apply the principle of least privilege to restrict access to only what's necessary.
iii. Require management approval for role changes and access requests.
iv. Conduct quarterly role audits for high-risk users.

5. Just-In-Time (JIT) Privileged Access

i. Implement JIT privilege elevation, allowing temporary access to elevated permissions based on:
    - Ticket numbers or approvals
    - Expiration timers
    - Session recording and auditing

ii. Automatically revoke privileges after task completion.

6. Privileged Access Workstations (PAWs)

Privileged Access Workstations (PAWs) are hardened and dedicated endpoints used exclusively for conducting administrative and sensitive operations involving State Data and CJI. They are a critical component of a tiered access model that separates high-risk functions from general-purpose computing environments. Require the use of dedicated, hardened PAWs for all administrative and high-privilege tasks.

i. Privileged Access Workstations (PAWs) must:

    - Be isolated from internet access and general use
    - Enforce full disk encryption and application whitelisting
    - Log and monitor all activities

ii. Prevent lateral movement by limiting PAW connectivity to high-trust zones only.

iii. Privileged Access Workstations (PAWs) Client-Side Policies

    - Dedicated Use Only - Prohibit general use (e.g., email, web browsing, document editing) on PAWs. Access must be limited to approved administrative tools and portals.
    - Application Whitelisting - Use application control to allow only pre-approved software (e.g., via Microsoft AppLocker or equivalent).
    - Full Disk Encryption - Enable full disk encryption using FIPS 140-2 validated encryption methods (e.g., BitLocker or LUKS).
    - No External Media Access - Disable USB and removable media ports unless explicitly authorized and encrypted.

- Local Administrator Accounts Disabled - Users must authenticate through centralized, logged accounts; local admin use is prohibited.
- Endpoint Detection & Response (EDR) - Deploy EDR solutions to monitor, detect, and respond to threats in real time.
- Secure Boot & BIOS Passwords - Lock down boot options and apply BIOS/UEFI passwords to prevent tampering.
- Session Logging - Enable screen recording or detailed keystroke/session logging for all PAW activity.
- No Internet Access - Configure PAWs to route traffic only through approved management and administrative networks.

iv. Privileged Access Workstations (PAWs) Server-Side Policies

- Group Policy Objects (GPOs) - Apply GPOs to enforce baseline security settings, such as:
- Credential Guard - Windows Defender Exploit Guard
- Firewall rules - Login restrictions (Smart Card or MFA only)
- Network Access Control (NAC) - Restrict PAW access only to necessary administrative servers (e.g., domain controllers, SIEMs) via VLAN or SDN segmentation.
- Privileged Access Management (PAM) Integration - Integrate with PAM systems to control access to sensitive systems, enforce JIT access, and require approval workflows.
- Centralized Logging and SIEM - Forward all PAW logs (authentication, file access, changes) to a SIEM for correlation and alerting.
- Conditional Access Policies - Use Identity Providers (IdPs) to apply conditional access rules to Only allow access from PAW-tagged devices and Enforce device compliance and user risk evaluation
- Patch Management & Configuration Baselines - Ensure PAWs are centrally patched and regularly scanned for compliance with secure baselines (e.g., CIS benchmarks).
- Change Monitoring - Use Endpoint Threat Detection tools to monitor unauthorized changes or unapproved software.

7. Federated Identity & Single Sign-On (SSO)

i. Deploy SSO to streamline access and reduce password fatigue.
ii. Use federated identity protocols (SAML 2.0, OIDC, WS-Fed) for secure cross-domain authentication.
iii. Monitor federation trust relationships and validate assertions.

8. Logging, Auditing, and Alerting

i. Log all access attempts, authentication failures, privilege elevations, and identity lifecycle changes.
ii. Use SIEM platforms to:
    - Detect anomalous behavior
    - Correlate identity-related events
    - Trigger alerts and incident response

9. Insider Threat Detection

i. Implement User and Entity Behavior Analytics (UEBA) to detect suspicious activity.
ii. Monitor identity-based threat indicators:
    - Access to unusual resources
    - Time-of-day anomalies
    - Excessive file downloads or privilege use
iii. Use decoy assets (honeytokens) to lure and detect unauthorized users.

10. Governance, Risk, and Compliance (GRC)

i. Integrate IAM with GRC platforms for:
    - Real-time compliance reporting
    - Automated control validation
    - Risk-based access decisions
ii. Map IAM controls frameworks such as:
    - NIST 800-53 (AC, IA control families)
    - FBI CJIS Security Policy
    - FISMA and Privacy Act

14. APPENDIX H: Security Addendum

This Security Addendum, appended to and incorporated by reference in a CJIS-CT and private sector contract entered into for such purpose, is intended to ensure that the benefits of privatization are not attained with any accompanying degradation in the security of the CJIS-CT system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security.

CJIS-CT may privatize functions traditionally performed under a management control agreement, subject to the terms of this Security Addendum. Access by a private contractor's personnel to State data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the CJIS-CT's function and the focus of the contract. The contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by CJIS-CT.

EXAMPLE OF A CONTRACT ADDENDUM

AMENDMENT NO. TO THE CONTRACT BETWEEN CJIS-CT AND PRIVATE PARTY ENTERED INTO [DATE]

CJIS-CT and PRIVATE PARTY, upon notification and pursuant to Paragraph/Section No. [the amendment clause of the original contract] of that certain contract entered into by these parties on [date][and entitled "_"], hereby amend and revise the contract to include the following:

1. Access to and use of criminal history record information and other sensitive information maintained in CJIS-CT managed criminal justice information systems by PRIVATE PARTY are subject to the following restrictions:

a.

b.

c.

and

d. The Security Addendum appended hereto, which is incorporated by reference and made a part thereof as if fully appearing herein.

This amendment is effective the ____ day of _________, 20__.
On behalf of CJIS-CT

Printed Name Title

Signature Date

On behalf of PRIVATE PARTY:

Printed Name Title

Signature Date

CJIS-CT INFORMATION SERVICES

SECURITY ADDENDUM

(Check with CJIS-CT ISO for the latest version of the Security Addendum)

The goal of this document is to augment the CJIS-CT Security Policy to ensure adequate security is provided for CJIS-CT Information systems while
(1) under the control or management of a private entity or
(2) connectivity to CJIS-CT Information systems has been provided to a private entity (contractor).
Adequate security is defined as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of State Data and CJI information."
The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS-CT Security Policy in effect when the contract is executed), as well as with policies and standards established by the FBI CJIS Security Policy.
This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the CJIS-CT information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, data security, and technical security.
The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of CJIS-CT.

1.00 Definitions
1.01 CJIS-CT which enters into an agreement with a private contractor subject to this Security Addendum.
1.02 Contractor – a private business, organization or individual which has entered into an agreement with CJIS-CT
2.00 Responsibilities of CJIS-CT
2.01 CJIS-CT will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS-CT Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the Contractor and available for audit purposes. The acknowledgement may be signed by hand or via digital signature.
3.00 Responsibilities of the Contractor.
3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS-CT Security Policy in effect when the contract is executed and all subsequent versions), as well as FBI CJIS Security Policy.
4.00 Security Violations.

4.01 CJIS-CT must report security Incidents and violations to the State CSO along with indications of actions taken by CJIS-CT and Contractor.
4.02 Security violations can justify termination of the appended agreement.
4.03 Upon notification, the CJIS-CT reserves the right to:
a. Investigate or decline to investigate any report of unauthorized use;
b. Suspend or terminate access and services, including telecommunications links.

Access and services will be reinstated only after satisfactory assurances have been provided to the CJIS-CT. Upon termination, the Contractor's records containing CJIS-CT data must be deleted or returned.

5.00 Audit
5.01 CJIS-CT is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.
6.00 Scope and Authority
6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor and CJIS-CT
6.02 The following documents are incorporated by reference and made part of this agreement:
(1) Security Addendum
(2) CJIS-CT Security Policy;
6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS-CT Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.
6.04 This Security Addendum may only be modified by CJIS-CT.
6.05 All notices and correspondence shall be forwarded by mail to

Executive Director
State of Connecticut
Criminal Justice Information System (CJIS-CT) - Governing Board
55 Farmington Ave, 11th floor
Hartford, CT 06105 |

CJIS-CT SECURITY ADDENDUM
CERTIFICATION

(Check with CJIS-CT ISO for the latest version of the Security Addendum)

I hereby certify that I am familiar with the contents of
(1) Security Addendum, including its legal authority and purpose.
(2) CJIS-CT Security Policy; and agree to be bound by their provisions.

I recognize that State Data and CJI, by their very nature, are sensitive and has potential for great harm if misused. I acknowledge that access to State Data and CJI is therefore limited to the purpose(s) for which CJIS-CT has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_______________________________________ _______________
Printed Name/Signature of Contractor Employee Date

_______________________________________ _______________
Printed Name/Signature of Contractor Representative Date

Organization and Title of Contractor Representative

15. APPENDIX I: Statutes

Sec. 54-142q. Criminal Justice Information System Governing Board. Membership. Duties and responsibilities. Access to information. (a) As used in this section, (1) "governing board" means the Criminal Justice Information System Governing Board established in this section, (2) "offender-based tracking system" means an information system that enables, as determined by the governing board and subject to this chapter, criminal justice agencies, as defined in subsection (b) of section 54-142g, the Division of Public Defender Services and the Office of the Federal Public Defender to share criminal history record information, as defined in subsection (a) of section 54-142g, and to access electronically maintained offender and case data involving felonies, misdemeanors, violations, motor vehicle violations, motor vehicle offenses for which a sentence to a term of imprisonment may be imposed, and infractions, and (3) "criminal justice information systems" means the information systems designed and implemented pursuant to section 54-142s.

(b) There shall be a Criminal Justice Information System Governing Board which shall be within the Department of Emergency Services and Public Protection for administrative purposes only and shall oversee criminal justice information systems.

(c) The governing board shall be composed of the Chief Court Administrator, the Commissioner of Emergency Services and Public Protection, the Secretary of the Office of Policy and Management, the Commissioner of Correction, the chairperson of the Board of Pardons and Paroles, the Chief State's Attorney, the Chief Public Defender, the Commissioner of Administrative Services, the Victim Advocate, the Commissioner of Motor Vehicles, the chairpersons and ranking members of the joint standing committee of the General Assembly on judiciary and the president of the Connecticut Police Chiefs Association. The Chief Court Administrator and a person appointed by the Governor from among the membership shall serve as cochairpersons. Each member of the governing board may appoint a designee who shall have the same powers as such member.

(d) The governing board shall meet at least once during each calendar quarter and at such other times as the chairperson deems necessary. A majority of the members shall constitute a quorum for the transaction of business.

(e) The governing board shall hire an executive director of the board who shall not be a member of the board and who shall serve at the pleasure of the board. The executive director shall be qualified by education, training or experience to oversee the design and implementation of a comprehensive, state-wide information technology system for the sharing of criminal justice information as provided in section 54-142s. The Department of Emergency Services and Public Protection shall provide office space and such staff, supplies and services as necessary for the executive director to properly carry out his or her duties under this subsection.

(f) The governing board shall develop plans, maintain policies and provide direction for the efficient operation and integration of criminal justice information systems, whether such systems service a single agency or multiple agencies. The governing board shall establish standards and procedures for use by agencies to assure the interoperability of such systems, authorized access to such systems and the security of such systems.

(g) In addition to the requirements of subsection (f) of this section, the duties and responsibilities of the governing board shall be to: (1) Oversee the operations and administration of criminal justice information systems; (2) establish such permanent and ad hoc committees as it deems necessary, with appointments to such committees not restricted to criminal justice agencies; (3) recommend any legislation necessary for implementation, operation and maintenance of criminal justice information systems; (4) establish and implement policies and procedures to meet the system-wide objectives, including the provision of appropriate controls for data access and security and (5) perform all necessary functions to facilitate the coordination and integration of criminal justice information systems.

(h) A member of the governing board, a member of a permanent or an ad hoc committee established by the governing board, and any person operating and administering the criminal justice information system shall be deemed to be “state officers and employees” for the purposes of chapter 53 and section 5-141d.

(i) Information that may be accessed by the Division of Public Defender Services or the Office of the Federal Public Defender pursuant to subsection (a) of this section shall be limited to: (1) Conviction information, as defined in subsection (c) of section 54-142g, (2) information that is otherwise available to the public, and (3) information, including nonconviction information, concerning a client whom the division has been appointed by the court to represent and is representing at the time of the request for access to such information.

(P.A. 99-14, S. 1, 2; P.A. 00-20, S. 2–4; P.A. 04-219, S. 24; 04-234, S. 2; P.A. 05-178, S. 1; June Sp. Sess. P.A. 07-4, S. 25; Jan. Sp. Sess. P.A. 08-1, S. 39; P.A. 09-26, S. 1; P.A. 11-51, S. 76, 181; June Sp. Sess. P.A. 17-2, S. 100, 101, 103, 104.)

History: P.A. 99-14 effective May 12, 1999; P.A. 00-20 amended Subsec. (a) to authorize the Division of Public Defender Services to participate in the offender-based tracking system and added Subsec. (f) to limit the types of information that the division may access, effective April 25, 2000; P.A. 04-219 amended Subsec. (b) to add the Commissioner of Emergency Management and Homeland Security, effective January 1, 2005; P.A. 04-234 replaced Board of Pardons and Board of Parole with Board of Pardons and Paroles, effective July 1, 2004; P.A. 05-178 inserted definitions of “governing board” and “offender-based tracking system” as new Subsec. (a), redesignated existing Subsecs. (a) to (f) as Subsecs. (b) to (g) and amended redesignated Subsec. (b) to require that governing board be within the Office of Policy and Management for administrative purposes only, to delete definition of “offender-based tracking system” and to make technical changes; June Sp. Sess. P.A. 07-4 amended Subsec. (a) to redefine “offender-based tracking system” in Subdiv. (2) and add Subdiv. (3) defining “criminal justice information systems”, amended Subsec. (b) to provide that board “shall oversee criminal justice information systems” and delete language re information system, added new Subsec. (e) to require board to develop plans, maintain policies and provide direction for the efficient operation and integration of criminal justice information systems and establish standards and procedures re interoperability of, access to and security of such systems, redesignated existing Subsecs. (e), (f) and (g) as Subsecs. (f), (g) and (h), and amended Subsec. (f) to provide that duties and responsibilities enumerated are “In addition to the requirements of subsection (e) of this section” and replace “offender-based tracking system” with “criminal justice information systems”; Jan. Sp. Sess. P.A. 08-1 amended Subsec. (c) to replace provision re Chief Court Administrator shall serve as chairperson with provision re Chief Court Administrator and person appointed by the Governor from among the membership shall serve as cochairpersons and add chairpersons and ranking members of the judiciary committee as members of governing board, added new Subsec. (e) re hiring and qualifications of an executive director and the provision of office space, staff, supplies and services for executive director to carry out his or her duties, redesignated existing Subsecs. (e) to (h) as new Subsecs. (f) to (i), and made a technical change in new Subsec. (g), effective January 25, 2008; P.A. 09-26 referenced the Office of the Federal Public Defender in Subsecs. (a) and (i) and made a technical change; P.A. 11-51 amended Subsec. (c) to replace "Commissioner of Public Safety" and "Commissioner of Emergency Management and Homeland Security" with "Commissioner of Emergency Services and Public Protection", effective July 1, 2011; pursuant to P.A. 11-51, "Chief Information Officer of the Department of Information Technology" was changed editorially by the Revisors to "Commissioner of Administrative Services", effective July 1, 2011; June Sp. Sess. P.A. 17-2 amended Subsec. (a)(3) to redefine "criminal justice information systems", amended Subsec. (b) to replace "Office of Policy and Management" with "Department of Emergency Services and Public Protection", amended Subsec. (e) to replace "Office of Policy and Management" with "Department of Emergency Services and Public Protection", and amended Subsec. (h) to replace "offender-based tracking system" with "criminal justice information system", effective October 31, 2017.*See Sec. 4-38 for definition of "administrative purposes only".*

Sec. 54-142r. Availability of data in criminal justice information system. Procedures for obtaining data. (a) Any data in a criminal justice information system, as defined in section 54-142q, shall be available to the Commissioner of Administrative Services and the executive director of a division of or unit within the Judicial Department that oversees information technology, or to such persons' designees, for the purpose of maintaining and administering said system.

(b) Any data in said system from an information system of a criminal justice agency, as defined in subsection (b) of section 54-142g, that is available to the public under the provisions of the Freedom of Information Act, as defined in section 1-200, shall be obtained from the agency from which such data originated. The Commissioner of Emergency Services and Public Protection shall provide to any person who submits a request for such data to the Criminal Justice Information System Governing Board, pursuant to said act, the name and address of the agency from which such data originated.

(P.A. 05-178, S. 2; P.A. 06-196, S. 187; P.A. 11-51, S. 76; June Sp. Sess. P.A. 17-2, S. 102, 105.)

History: P.A. 06-196 made technical changes, effective June 7, 2006; pursuant to P.A. 11-51, "Chief Information Officer of the Department of Information Technology" was changed editorially by the Revisors to "Commissioner of Administrative Services" in Subsec. (a), effective July 1, 2011; June Sp. Sess. P.A. 17-2 amended Subsec. (a) to replace "the offender-based tracking system" with "a criminal justice information system" and amended Subsec. (b) to replace "Secretary of the Office of Policy and Management" with "Commissioner of Emergency Services and Public Protection", effective October 31, 2017.

Sec. 54-142s. State-wide information technology system for sharing of criminal justice information. (a) The Criminal Justice Information System Governing Board shall design and implement a comprehensive, state-wide information technology system to facilitate the immediate, seamless and comprehensive sharing of information between all state agencies, departments, boards and commissions having any cognizance over matters relating to law enforcement and criminal justice, and organized local police departments and law enforcement officials.

(b) Such information technology system shall include, without limitation, a central tracking and information database, a central electronic document repository and centralized analytical tools, as provided in subsections (c) to (e), inclusive, of this section, all of which shall be developed with state-of-the-art technology, as provided in subsection (f) of this section, and such other components or elements as are determined to be appropriate or necessary by the board after development of a plan for the design and implementation of such system.

(c) Such information technology system shall include a central, integrated criminal justice tracking and information database that provides:

(1) Complete biographical information and vital statistics for all offenders and former offenders still living.

(2) Tracking information for all offenders in the criminal justice system, from investigation through incarceration and release, and seamless integration with any electronic monitoring systems, global positioning systems (GPS) and any offender registries.

(d) Such information technology system shall include a central, integrated electronic repository of criminal justice records and documents that provides:

(1) Access to all state and local police reports, presentence investigations and reports, psychological and medical reports, criminal records, incarceration and parole records, and court records and transcripts, whether such records and documents normally exist in electronic or hard copy form.

(2) Access to scanning and processing facilities to ensure that such records and documents are integrated into the system and updated immediately.

(e) Such information technology system shall include centralized analytical tools, bundled together in a custom-designed enterprise system that includes:

(1) Analytical tools that empower and enhance criminal case assessment, sentencing and plea agreement analysis and pardon, parole, probation and release decisions;

(2) Analytical tools that empower and enhance forecasting concerning recidivism and future offenses for each individual offender.

(3) Collaborative functionality that enables seamless cross-department communication, information exchange, central note-taking and comment capabilities for each offender.

(f) Such information technology system shall be developed with state-of-the-art relational database technology and other appropriate software applications and hardware, and shall be:

(1) Completely accessible by any authorized criminal justice official through the Internet;

(2) Completely integrated with the state police, organized local police departments, law enforcement agencies and such other agencies and organizations as the governing board deems necessary and appropriate, and their information systems and database applications;

(3) Indexed and cross-referenced by offender name, residence, community, criminal offense and any other data points necessary for the effective administration of the state's criminal justice system;

(4) Fully text searchable for all records;

(5) Secure and protected by high-level security and controls;

(6) Accessible to the public subject to appropriate privacy protections and controls.

(7) Monitored and administered by the Criminal Justice Information Systems Governing Board, with the assistance of the Department of Administrative Services, provided major software and hardware needs may be provided and serviced by private, third-party vendors.

(g) Not later than July 1, 2008, the Criminal Justice Information Systems Governing Board shall issue a request for proposals for the design and implementation of such information technology system and hire a consultant to develop a plan for such design and implementation.

(h) Not later than July 1, 2008, and not later than January first and July first of each year thereafter, the Criminal Justice Information System Governing Board shall submit a report, in accordance with section 11-4a, to the joint standing committees of the General Assembly having cognizance of matters relating to criminal justice and appropriations and the budgets of state agencies concerning the status of the design and implementation of such information technology system. In conjunction with the report submitted not later than January first of each year, the board shall also make a presentation to said committees during the ensuing regular session concerning the status of the design and implementation of such information technology system and a specific itemization of the additional resources, if any, that are needed to achieve such design and implementation.

16. APPENDIX J: References

1. FBI CJIS Security Policy Version 6.0, December 2024
2. NIST SP 800-18 Rev. 1 – Guide for Developing Security Plans for Federal Information Systems
3. NIST SP 800-30 Rev. 1 – Guide for Conducting Risk Assessments
4. NIST SP 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
5. NIST SP 800-39 – Managing Information Security Risk: Organization, Mission, and Information System View
6. NIST SP 800-47 – Security Guide for Interconnecting Information Technology Systems
7. NIST SP 800-50 – Building an Information Technology Security Awareness and Training Program
8. NIST SP 800-52 Rev. 2 – Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
9. NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations
10. NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide
11. NIST SP 800-63-3 – Digital Identity Guidelines
12. NIST SP 800-88 Rev. 1 – Guidelines for Media Sanitization
13. NIST SP 800-92 – Guide to Computer Security Log Management
14. NIST SP 800-113 – Guide to SSL VPNs
15. NIST SP 800-124 Rev. 2 – Guidelines for Managing the Security of Mobile Devices in the Enterprise
16. NIST SP 800-128 – Guide for Security-Focused Configuration Management of Information Systems
17. NIST SP 800-137 – Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
18. NIST SP 800-161 Rev. 1 – Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
19. NIST SP 800-171 Rev. 2 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations