CT CJIS Security Policy v. 1.0

Approved by the CJIS Governing Board on October 16, 2014

CT CJIS Security Policy v. 1.0

Prepared by the CT CJIS Security Workgroup:

Phil Conen
David Dove
Chris Duryea
James Harris
Darryl Hayes
John Russotto
Sean Thakkar
Terry Walker
Steven Wallick
Antoinette Webster

For

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

Table of Contents

Terminology Used in This Document

The following is a list of terms and abbreviations that are used throughout this document, for purposes of this document, along with definitions or references that help define the term or abbreviation. The Dictionary of Terms contains an additional list of terms and abbreviations.

- The term "agency" means all entities specified or referenced under sections **54-142q(a)(2), 54-142r, and 54-142s(a)** of the general statutes.
- The term "applicant" means any person or entity that is requesting access to CISS information.
- The term "CJIS" means the Connecticut Criminal Justice Information System, for purposes of this document.
- The term "CJI" means criminal justice information. The term, "Non CJI" means non-criminal justice information. Both terms refer to criminal justice information in the state of Connecticut.
- Connecticut Information Sharing System (CISS) refers to the statewide information technology system designed in support of section **54-142s** of the general statutes, the offender-based tracking system designed in support of section **54-142q** of the general statutes (commonly referred to as "OBTS"), the Connecticut Impaired Driver Records Information system (commonly referred to as "CIDRIS"), and other information technology systems that may be designed and implemented in accordance with **54-142s** of the general statutes.
- The term "CISS State Data" refers to all computerized image, audio, and video files and other information contained within CISS. "CISS State Data" *does not* refer to information that is subject to the FBI CJIS Security Policy unless otherwise specified. Certain CISS State Data may be subject to additional security measures or protections that may not be covered in this document.
- The Connecticut Criminal Justice Information System Governing Board will be hereinafter referred to as the "CJIS Governing Board." The CJIS Governing Board is defined under section **54-142q** of the general statutes.

1. 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 Governing Board authorized that the Criminal Justice Information System (CJIS) to update and expand the existing security policy approved in 2005. 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 CT CJIS 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 Data. It includes agency self-assessment and certification tools designed to minimize the administrative burden on both CT CJIS and the agencies.

The CT CJIS Security Policy is meant to:

- Allow agencies access to CISS State Data while providing appropriate controls to protect the full lifecycle of CISS State Data
- Stand as a baseline policy for those agencies that cannot or do not wish to meet the more stringent requirements of the FBI CJIS Security Policy v. 5.3
- Provide guidance for the viewing, transmission, dissemination, storage, and destruction of CISS State 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 *does not* authorize access to FBI data.

The CT CJIS Security Policy will be periodically updated to reflect the security requirements of evolving business models. It features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists CT CJIS with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CT CJIS 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 noncriminal justice communities.

2. Introduction

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

2.1. 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 to ensure continuity of information protection, for information both at rest and in transit.

The CT CJIS 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) and information and to protect and safeguard CT criminal justice information and CT non-criminal justice information. This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CT CJIS 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.

2.2. Scope

By the authority vested in the Governing Board through sections **54-142q** through **54-142s** of the general statutes, the CJIS 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 CISS 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 CISS Security Policy does not supersede or replace the FBI CJIS Security Policy to the extent that the FBI CJIS Security Policy applies to CISS or CISS State Data.

2.3. Relationship to Local Security Policy and Other Policies

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

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CT CJIS 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 CT CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required by the CJIS Governing Board.

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

Appendix I contains the Wireless Access Best Practices, Appendix II contains Security Incident Response, and Appendix V and Appendix VI lists the security compliance forms referenced in this document.

2.4. Administration

The CISS Security Policy shall only be amended or changed by the Governing Board.

Until such time as another administrative body is established by the CJIS Governing Board to maintain the CISS Security Policy, the State of Connecticut's **Chief Security Officer** (CSO) or the CSO's designee shall meet quarterly, or more frequently if necessary, with representatives from all of the agencies to review, clarify, and propose amendments to the CISS Security Policy.

2.5. Distribution of the CT CJIS Security Policy

The CT CJIS Security Policy, Version 1.0 and later, is a publically available document and may be posted and shared without restrictions.

3. The CT CJIS Security Policy Approach

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

3.1. CT CJIS Security Policy Vision Statement

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

3.2. Architecture Independent

The CT CJIS 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 CT CJIS with the flexibility for tuning the information security infrastructure and policies to reflect their own environments.

3.3. Risk versus Realism

Every “shall” statement contained within the CT CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CT CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency-specific risks.

4. Roles and Responsibilities

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

4.1. 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 CT CJIS and its user community. This section provides a description of the following entities and roles:

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

4.1.1. CJIS Governing Board

The CJIS 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 Office of Policy and Management for administrative purposes only and shall oversee criminal justice information systems.”

Also in section 54-142q, “The CJIS 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.”

4.1.2. CJIS Executive Director

The CJIS Executive Director is an individual designated by the CJIS Governing Board as responsible for the administration of the CT CJIS network for the Governing Board except where FBI data is transported or stored. The role of CJIS Executive Director shall not be outsourced. The CJIS Executive Director may delegate responsibilities to subordinate agencies. The CJIS 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 CT CJIS systems used to process, store, or transmit CJI and Non CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
  - Ensure appropriate use, enforce system discipline, and ensure CT CJIS 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 Governing Board.
  - Ensure the appointment of the CJIS **Information Security Officer** (ISO) and determine the extent of authority to the CJIS ISO.
  - The CJIS Executive Director, or designee, shall ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CT CJIS systems.
  - Ensure each agency having access to CJI has someone designated as the **Local Agency Security Officer** (LASO).
  - Approve access to CT CJIS systems after reviewing the CT CJIS Forms 1 and 2.
  - Assume ultimate responsibility for managing the security of CT CJIS systems within their state and/or agency.
  - Perform other related duties outlined by the user agreements with the CT CJIS.

4.1.3. CT Terminal Agency Coordinator (TAC)

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

4.1.4. 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.

4.1.5. 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.

4.1.6. CJIS Information Security Officer

The CJIS Information Security Officer (ISO) shall:

- Document technical compliance with the CT CJIS 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 CT CJIS security-related controls for the CJA.
- Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CJIS Governing Board, the affected criminal justice agency, and the DAS/BEST ISO major incidents that significantly endanger the security or integrity of CJI and Non CJI.

4.1.7. 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 including managing indexes, backup/restore, configuration of system files, etc.
- Respond to automated system alerts or other problems and take corrective action as necessary.

4.1.8. Local Agency Security Officer

Each Local Agency Security Officer (LASO) shall:

- Identify who is using the CJIS 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 CT CJIS 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 Governing Board ISO is promptly informed of security incidents.

4.1.9. CISS Community Agency Administrator

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

5. CISS State Data and Personally Identifiable Information

5.1. CISS State Data

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 to ensure continuity of information protection, for information both at rest and in transit.

CISS State Data is the term used to refer to all of the CT 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, except that "CISS State Data" does not refer to information that is subject to the FBI CJIS Security Policy unless otherwise specified.

As stated specified in the definition above, CISS State data generally does not include information that is subject to the FBI CJIS Security Policy, and this categorization may assist with protecting and safeguarding CISS State data that is exchanged with criminal justice agencies outside the CISS architecture.

The five categories are described in more detail below:

- 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.

5.1.1. CISS State Data Sources

The data sources for CISS include the following:

- OBIS
- PRAWN
- CRMVS
- MNI/CCH
- COLLECT
- WEAPONS
- CMIS
- BOPP
- OBTS
- POR

- PSI
- SOR
- CIB
- DMV

5.2. Access, Use and Dissemination of CISS State Data

5.2.1. Storage

When CISS State Data is stored, agencies shall establish consistent with Ct. General Statutes administrative, technical and physical safeguards to ensure the security and confidentiality of the information. Justification and Penalties

5.2.1.1. Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all inquiries.

5.2.1.2. Penalties

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

5.3. Commercial Distribution of CISS State Data

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

6. Policy and Implementation

The policy areas focus upon the data and services that the CT CJIS 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 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:

- **Policy Area 1—Information Exchange Agreements**
- **Policy Area 2—Security Awareness Training**
- **Policy Area 3—Incident Response**
- **Policy Area 4—Auditing and Accountability**
- **Policy Area 5—Access Control**
- **Policy Area 6—Identification and Authentication**
- **Policy Area 7—Configuration Management**
- **Policy Area 8—Media Protection**
- **Policy Area 9—Physical Protection**
- **Policy Area 10— System and Information Integrity Policy and Procedures**
- **Policy Area 11—Formal Audits**
- **Policy Area 12—Personnel Security**

6.1. 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.

6.1.1. Information Exchange

Information exchanges shall be supported by documentation committing all parties to the terms of information exchange. As described in the Integration Design Documents.

6.1.1.1. 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 CISS State Data. These procedures apply to the exchange of CISS State Data no matter the form of exchange.

The policies for information handling and protection also apply to using CISS State 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.

6.1.2. Connecticut Justice Information System Security Compliance Assessment Form (CT CJIS-2)

The Connecticut Justice Information System Security Compliance Assessment Form (CT CJIS-2) is used as a mechanism for municipalities, state and federal agencies to assess their compliance with the CT CJIS Security Requirements and Recommendations as adopted by the Connecticut CJIS Governing Board.

6.1.3. Connecticut Justice Information System Security Compliance Certification Form (CT CJIS-3)

The Connecticut Justice Information System Security Compliance Certification Form (CT CJIS-3) is used as a mechanism for municipalities, state and federal agencies to certify their compliance with the CT CJIS Security Requirements and Recommendations as adopted by the Connecticut CJIS Governing Board.

6.1.4. Secondary Dissemination

CISS will log all dissemination of data.

6.2. Policy Area 2: Security Awareness Training

Basic security awareness training shall be required within six (6) months of initial assignment, and triennially thereafter, for all personnel who have access to CISS State Data. The CJIS Executive Director may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from such agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

6.2.1. Awareness Topics

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

6.2.1.1. All Personnel

At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to Data:

- Rules that describe responsibilities and expected behavior with regard to Data usage.
- Implications of noncompliance.
- Incident response (points of contact; individual actions).
- Media protection.
- Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
- Protect information subject to confidentiality concerns — hardcopy through destruction.
- Proper handling and marking of Data.
- Threats, vulnerabilities, and risks associated with handling of Data.
- Social engineering.

- Dissemination and destruction.

6.2.1.2. Personnel with Physical and Logical Access

In addition to topics mentioned in All Personnel above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to Data:

- Rules that describe responsibilities and expected behavior with regard to information system usage.
- Password usage and management—including creation, frequency of changes, and protection.
- Protection from viruses, worms, **Trojan horses**, and other malicious code.
- Unknown e-mail/attachments.
- Web usage—allowed versus prohibited; monitoring of user activity.
- Spam.
- Physical security—increases in risks to systems and data.
- Handheld device security issues—address both physical and wireless security issues.
- Use of **encryption** and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
- Laptop security—address both physical and information security issues.
- Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
- Access control issues—address least privilege and separation of duties.
- Individual accountability—explain what this means in the agency.
- Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
- Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
- Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
- Threats, vulnerabilities, and risks associated with accessing CT CJIS Service systems and services.

6.2.1.3. Personnel with Information Technology Roles

In addition to All Personnel, Page 17, and Personnel with Physical and Logical Access, Page 18, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

- Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
- Data backup and storage—centralized or decentralized approach.
- Timely application of system patches—part of configuration management.
- Access control measures
- Network infrastructure protection measures

6.2.2. Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CJIS Executive Director. Maintenance of training records can be delegated to the local level.

6.3. Policy Area 3: Incident Response

There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile.

Agencies shall:

- Establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
- Track, document, and report incidents to appropriate agency officials and/or authorities.

Agency Security Officers have been identified as the **Point of Contact** (POC) on security-related issues for their respective agencies and upon determination of a local threat that rises to the level of a threat to CISS they shall institute the CT CJIS incident response reporting procedures at the local level.

Appendix IV contains a sample incident notification report for use when communicating the details of an incident to the CISS ISO.

6.3.1. Reporting Information Security Events

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

6.3.1.1. Reporting Structure and Responsibilities

6.3.1.1.1. CT CJIS Responsibilities

CT CJIS may:

- Manage and maintain the CT CJIS Computer Security Incident Response Capability (CSIRC).
- Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
- Ensure additional resources for all incidents affecting CT CJIS controlled systems as needed.
- Disseminate prompt advisories of system threats and operating system vulnerabilities.
- Track all reported incidents and/or trends.

- Monitor the resolution of all incidents.
- Create and maintain an email and contact distribution list for incident response and notification (i.e., utilize **Everbridge** for alerting personnel).

6.3.1.1.2. CJIS ISO Responsibilities

The CJIS ISO may:

- Assign individuals in each state and local, law enforcement organization to be the primary point of contact for interfacing with the CT CJIS concerning incident handling and response.
- Identify individuals who are responsible for reporting incidents within their area of responsibility.
- Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
- Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
- Act as a single POC for their jurisdictional area for requesting incident response assistance.

6.3.2. Incident Response Training

The CJIS ISO may ensure general incident response roles responsibilities are included as part of required security awareness training.

6.3.3. Incident Monitoring

The CJIS ISO shall track and document information system security incidents on an ongoing basis. The CJIS ISO shall maintain completed security incident reporting forms until the subsequent audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Refer to Appendix II, Page 33, for more information on Security Incident Response.

6.4. Policy Area 4: Auditing and Accountability

- CT CJIS will comply with the current FBI CJIS Security Policy for auditing and accountability.

6.5. Policy Area 5: Access Control

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

6.5.1. Account Management

CT CJIS shall manage information system accounts or profiles, including establishing, activating, modifying, reviewing, disabling, and removing accounts or profiles. CT CJIS 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. CT CJIS shall identify authorized users of the information system and specify access rights/privileges. CT CJIS shall grant access to the information system based on:

- Valid need-to-know/need-to-share that is determined by assigned official duties.
- Satisfaction of all personnel security criteria.

When CT CJIS is responsible for account management it shall be notified when:

- A user's information system usage or need-to-know or need-to-share changes.
- A user is terminated or transferred or associated accounts or profiles are removed, disabled, or otherwise secured.

6.5.2. 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.

6.5.2.1. Access Control Criteria

CT CJIS shall control access to CISS State Data based on one or more of the following:

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

6.5.2.2. Access Control Mechanisms

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

- **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.
- **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.

- **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.
- **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.

6.5.3. Unsuccessful Login Attempts to the CISS Portal

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

6.5.4. 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 use notification message shall, at a minimum, provide the following information:

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

The system use 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

6.5.5. 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.

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

6.5.5.1. Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CISS State Data unless the CT CJIS has established and documented the specific terms and conditions for personally owned information system usage. Devices must be from a list of CT CJIS approved 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).

6.5.5.2. Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CISS 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.

Refer to Appendix I, Page 30, for Wireless Access Best Practices.

6.6. Policy Area 6: Identification and Authentication

The agency 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.

6.6.1. Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CISS State Data shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CISS State Data or networks leveraged for CISS State 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.

6.6.1.1. Use of Agency Identifying Information in Transactions and Information Exchanges

An authorized originating agency identifier shall be used in each transaction on CT CJIS 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 CT CJIS shall be the Agency Identifying Information (AII), 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 AII. Servicing agencies may also use their own AII 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, CT CJIS shall ensure that the AII 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.**

6.6.2. Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. CT CJIS may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CISS State Data.

Each individual's identity shall be authenticated at either the local agency or CT CJIS level. The authentication strategy shall be part of the agency's audit for policy compliance. CT CJIS shall identify and authenticate all individuals who establish direct Web-based interactive sessions with CISS Services. The CISS shall authenticate the agency Identifier of all message-based sessions between the CT CJIS and its customer agencies but will not further authenticate the user, nor capture the unique identifier, for the originating operator because this function is performed at the local agency level.

6.6.2.1. Standard Authenticators

Authenticators are the something you know, something you are, or something you have part of the identification and authentication process. Examples of standard authenticators include passwords, tokens, biometrics, and personal identification numbers (PIN). In two factor authentication both factors cannot be the same.

6.6.2.1.1. Password

CISS shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:

- Be a minimum length of eight (8) characters on all systems.
- Not be a dictionary word or proper name.
- Not be the same as the Userid.
- Expire within a maximum of ninety (90) calendar days.
- Not be identical to the previous ten (10) passwords.
- Not be transmitted in the clear outside the secure location.
- Not be displayed when entered.

6.6.2.1.2. Personal Identification Number (PIN)

Refer to Appendix G-5 Personal Identification Number (PIN) for FBI best practices for the use of PINs.

6.7. Policy Area 7: Configuration Management

6.7.1. Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Policy Area 5: Access Control, Page 20, describes agency requirements for control of privileges and restrictions.

6.7.1.1. Least Functionality

The CT CJIS ISO shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

6.7.1.2. Network Diagram

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

The network topological drawing shall include the following:

- 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 end-point.
- 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.
- For Official Use Only markings.
- The date (day, month, and year) the drawing was created or updated.

6.7.2. Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g., descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) CT CJIS ISO shall protect the system documentation from unauthorized access consistent with the provisions as described in Policy Area 5: Access Control, Page 20.

6.8. Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

6.8.1. Media Storage and Access

CT CJIS ISO shall securely store electronic and physical media within physically secure locations or controlled areas. CT CJIS ISO shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted.

6.8.2. Media Transport

CT CJIS 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.

6.8.2.1. Electronic Media in Transit

“Electronic 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 electronic media containing CISS State 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.

6.8.2.2. Physical Media in Transit

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

6.8.3. Electronic Media Sanitization and Disposal

The CT CJIS ISO shall sanitize, that is, overwrite at least three (3) times or **degauss** electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). CT CJIS shall maintain written documentation of the steps taken to sanitize or destroy electronic media. CT CJIS ISO shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

6.8.4. Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

6.9. Policy Area 9: Physical Protection

All agencies shall carry out the duties for the physical protection of information system hardware, software, and media in accordance with sections 54-142h and 54-142i of the general statutes.

6.10. Policy Area 10: System and Information Integrity Policy and Procedures

6.10.1. Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

- Testing of appropriate patches before installation.
- Rollback capabilities when installing patches, updates, etc.
- Automatic updates without individual user intervention.
- Centralized patch management.
- Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

6.10.2. Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e., most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, **Trojan horses**) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

6.10.3. Spam and Spyware Protection

The agency shall implement **spam** and **spyware** protection.

The agency shall:

- Employ spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers).
- Employ spyware protection at workstations, servers and mobile computing devices on the network.
- Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., diskettes or compact disks) or other removable media as defined in this Policy.

6.11. Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

6.11.1. Audits by the CT CJIS

6.11.1.1. Triennial Compliance Audits by CT CJIS

CT CJIS is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. CT CJIS Audit Unit (CAU) shall conduct a triennial audit of each agency in order to verify compliance with applicable statutes, regulations and policies. This audit may include a sample of CJAs and, in coordination with the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

6.11.1.2. Triennial Security Audits by CT CJIS

CT CJIS is authorized to conduct security audits of the CT CJIS network and system once every three (3) years as a minimum to assess agency compliance with the CT CJIS Security Policy. This audit may include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CT CJIS Security Policy.

6.11.2. Special Security Inquiries and Audits

All agencies having access to CISS State Data shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the Security committee and shall include at least one representative of CT CJIS. All results of the inquiry and audit shall be reported to the Security committee with appropriate recommendations.

6.12. Policy Area 12: Personnel Security

All agencies shall carry out the duties for the security of personnel who have access to CISS State Data in accordance with section 54-142i of the general statutes.

6.12.1.1. Personnel Screening for Contractors and Vendors

Contractors and vendors shall meet the following requirements:

- Prior to granting access to CISS State Data, the CGA on whose behalf the Contractor is retained shall verify identification 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.
- 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.
- 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.
- A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified.
- Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
- The CGA shall maintain a list of personnel who have been authorized access to CISS State Data and shall, upon request, provide a current copy of the access list to the CT CJIS ISO.
- Applicants with a record of misdemeanor offense(s) may be granted access if the CT CJIS ISO determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The CGA may request the CT CJIS ISO to review a denial of access determination.

6.12.2. Personnel Termination

The agency, upon termination of individual employment, shall immediately terminate access to CISS State Data.

6.12.3. Personnel Transfer

The agency shall review CISS State Data access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts or profiles and changing system access authorizations.

6.12.4. Personnel Sanctions

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

Appendix I. Wireless Access Best Practices

The agency should:

- Establish usage restrictions and implementation guidance for wireless technologies
- 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.

Examples of wireless technologies include, but are not limited to: 802.11x, cellular networks. Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology, may require some additional security controls (see Appendix I). To be reviewed by sub-committee on a regular basis. Need to assess where, what type and why wireless access is necessary.

All 802.11x Wireless Protocols

Agencies should:

- 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.
- Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
- Place APs in secured areas to prevent unauthorized physical access and user manipulation.
- 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.
- Enable user authentication and encryption mechanisms for the management interface of the AP.
- Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with the Standard Authenticators, Page 24.
- 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.
- 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.
- Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.
- Ensure that encryption key sizes are at least 128 bits and the default shared keys are replaced by unique keys.
- Ensure that the ad hoc mode has been disabled unless the environment is such that the risk has been assessed and is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.
- Disable all nonessential management protocols on the APs and disable **hypertext transfer protocol** (HTTP) when not needed or protect HTTP access with authentication and encryption.

- Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
- Segregate, 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.
- 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.

Legacy 802.11 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 are to be used only if additional security controls are employed.
- Agencies shall follow the guidelines below regarding wireless implementation and cases where the WEP and WPA security features are used to provide wireless security in conjunction with the CT CJIS required minimum encryption specifications.
- Deploy **media access control** (MAC) **access control lists** (ACL); however, MAC ACLs do not represent a strong defense mechanism by themselves because they are transmitted in the clear from WLAN clients to APs so they can be captured easily.
- Enable WEP/WPA.
- Ensure the default shared keys are replaced by more secure unique keys.
- Enable utilization of key-mapping keys rather than default keys so that sessions are unique when using WEP.

Cellular

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), personal digital assistants (PDA), and “air cards” are examples of cellular handheld devices or devices that employ 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. Cellular devices are at risk due to a multitude of threats and consequently pose a risk to the enterprise.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

- Loss, theft, or disposal.
- Unauthorized access.
- Malware.
- Spam.
- Electronic eavesdropping.
- Electronic tracking (threat to security of data and safety of law enforcement officer).
- Cloning (not as prevalent with later generation cellular technologies).
- Server-resident data.

Cellular Risk Mitigations

Organizations shall, at a minimum, ensure that cellular devices:

- 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 Patch Management, Page 26.
- Are configured for local device authentication.
- Use advanced authentication.
- Encrypt all CISS data resident on the device.
- Erase cached information when session is terminated.
- Employ personal firewalls or run a **Mobile Device Management** (MDM) system that facilitates the ability to provide firewall services from the agency level.
- Employ antivirus software or run a MDM system that facilitates the ability to provide antivirus services from the agency level.

Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CISS data via voice is exempt from the encryption and authentication requirements when an officer determines there is an immediate need for the CISS data to further an investigation or situations affecting the safety of an officer or the general public.

Mobile Device Management (MDM)

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 (if so desired by the agency).

Devices that have been rooted, jailbroken, or have had any unauthorized changes made to them shall not be used to process, store, or transmit CISS State Data at any time. In addition to the security controls described in this Policy, agencies shall implement the following controls when allowing CISS State Data access from cell/smart phones and tablet devices:

- CISS State Data is only transferred between authorized applications and storage areas of the device.
- MDM with centralized administration capable of at least:
  - Remote locking of device
  - Remote wiping of device
  - Setting and locking device configuration
  - Detection of “rooted” and “**jailbroken**” devices
  - Enforcement of folder or disk level encryption

Personal Firewall

A personal firewall shall be employed on all devices that are mobile by design (i.e., laptops, handhelds, personal digital assistants, etc.). For the purpose of this Policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. At a minimum, the personal firewall shall perform the following activities:

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

Appendix II. Security Incident Response

Management of Information Security Incidents

A consistent and effective approach shall be applied to the management of information security incidents. Responsibilities and procedures shall be in place to handle information security events and weaknesses effectively once they have been reported.

Incident Handling

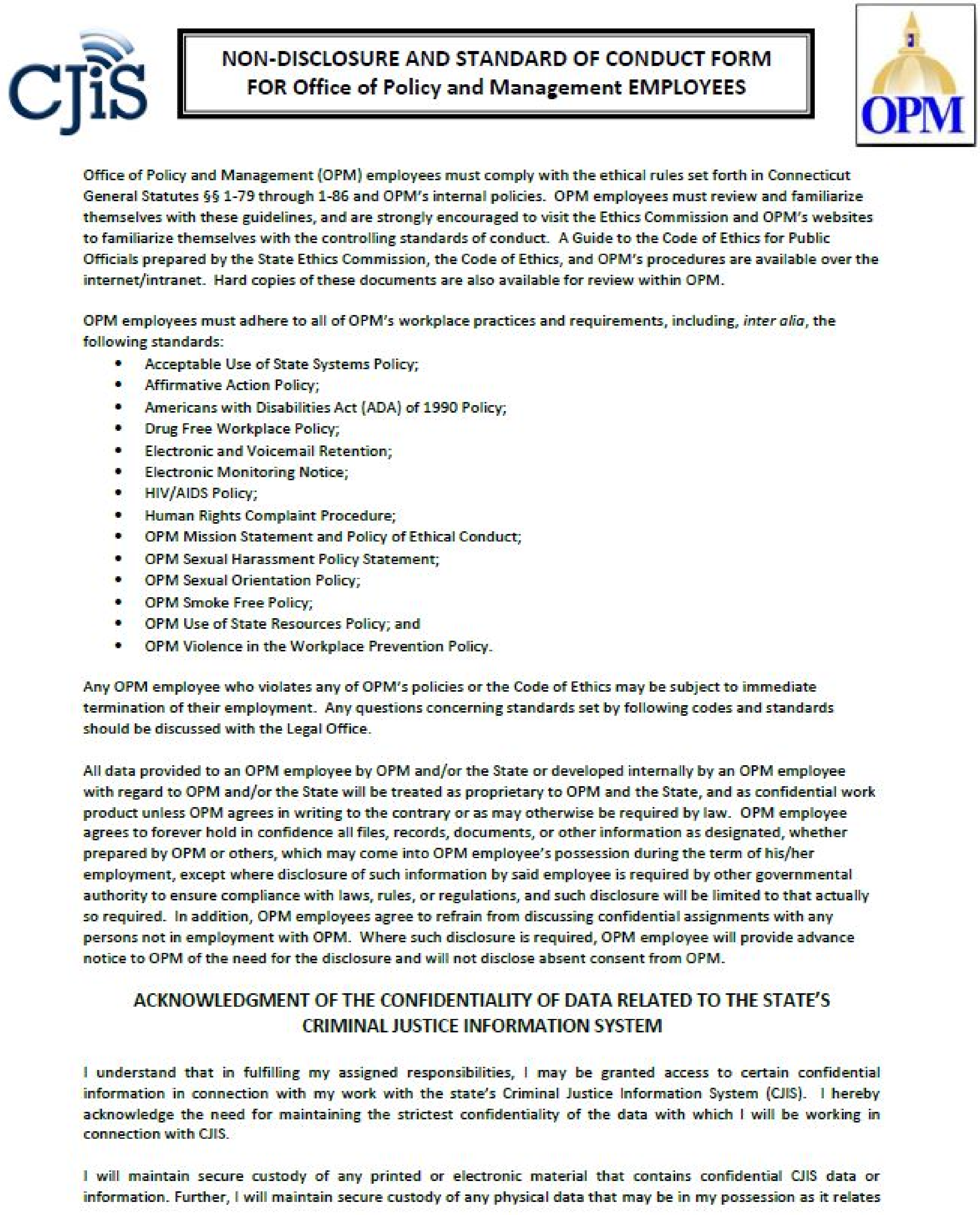
CISS may implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, CISS may employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. CISS should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

Collection of Evidence

Where a follow-up action against a party after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Appendix III. Non-Disclosure Agreements for Consultants



NON-DISCLOSURE AND STANDARD OF CONDUCT FORM FOR Office of Policy and Management EMPLOYEES

Office of Policy and Management (OPM) employees must comply with the ethical rules set forth in Connecticut General Statutes §§ 1-79 through 1-86 and OPM's internal policies. OPM employees must review and familiarize themselves with these guidelines, and are strongly encouraged to visit the Ethics Commission and OPM's websites to familiarize themselves with the controlling standards of conduct. A Guide to the Code of Ethics for Public Officials prepared by the State Ethics Commission, the Code of Ethics, and OPM's procedures are available over the internet/intranet. Hard copies of these documents are also available for review within OPM.

OPM employees must adhere to all of OPM's workplace practices and requirements, including, *inter alia*, the following standards:

- Acceptable Use of State Systems Policy;
- Affirmative Action Policy;
- Americans with Disabilities Act (ADA) of 1990 Policy;
- Drug Free Workplace Policy;
- Electronic and Voicemail Retention;
- Electronic Monitoring Notice;
- HIV/AIDS Policy;
- Human Rights Complaint Procedure;
- OPM Mission Statement and Policy of Ethical Conduct;
- OPM Sexual Harassment Policy Statement;
- OPM Sexual Orientation Policy;
- OPM Smoke Free Policy;
- OPM Use of State Resources Policy; and
- OPM Violence in the Workplace Prevention Policy.

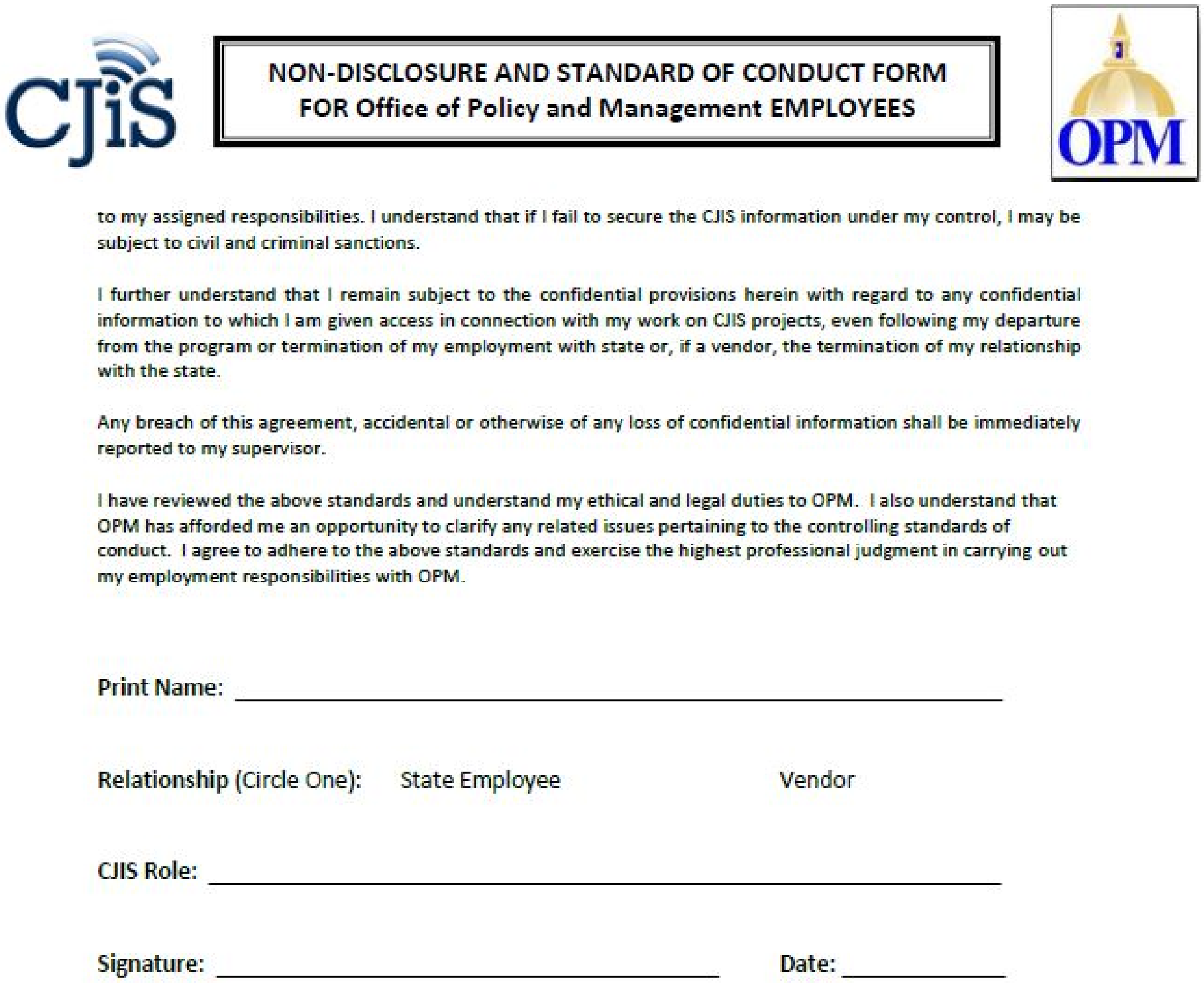
Any OPM employee who violates any of OPM's policies or the Code of Ethics may be subject to immediate termination of their employment. Any questions concerning standards set by following codes and standards should be discussed with the Legal Office.

All data provided to an OPM employee by OPM and/or the State or developed internally by an OPM employee with regard to OPM and/or the State will be treated as proprietary to OPM and the State, and as confidential work product unless OPM agrees in writing to the contrary or as may otherwise be required by law. OPM employee agrees to forever hold in confidence all files, records, documents, or other information as designated, whether prepared by OPM or others, which may come into OPM employee's possession during the term of his/her employment, except where disclosure of such information by said employee is required by other governmental authority to ensure compliance with laws, rules, or regulations, and such disclosure will be limited to that actually so required. In addition, OPM employees agree to refrain from discussing confidential assignments with any persons not in employment with OPM. Where such disclosure is required, OPM employee will provide advance notice to OPM of the need for the disclosure and will not disclose absent consent from OPM.

ACKNOWLEDGMENT OF THE CONFIDENTIALITY OF DATA RELATED TO THE STATE'S CRIMINAL JUSTICE INFORMATION SYSTEM

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 Criminal Justice Information System (CJIS). I hereby acknowledge the need for maintaining the strictest confidentiality of the data with which I will be working in connection with CJIS.

I will maintain secure custody of any printed or electronic material that contains confidential CJIS data or information. Further, I will maintain secure custody of any physical data that may be in my possession as it relates



NON-DISCLOSURE AND STANDARD OF CONDUCT FORM
FOR Office of Policy and Management EMPLOYEES

to my assigned responsibilities. I understand that if I fail to secure the CJIS 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 CJIS projects, even following my departure from the program or termination of my employment with state or, if a vendor, the termination of my relationship with the state.

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

I have reviewed the above standards and understand my ethical and legal duties to OPM. I also understand that OPM 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 OPM.

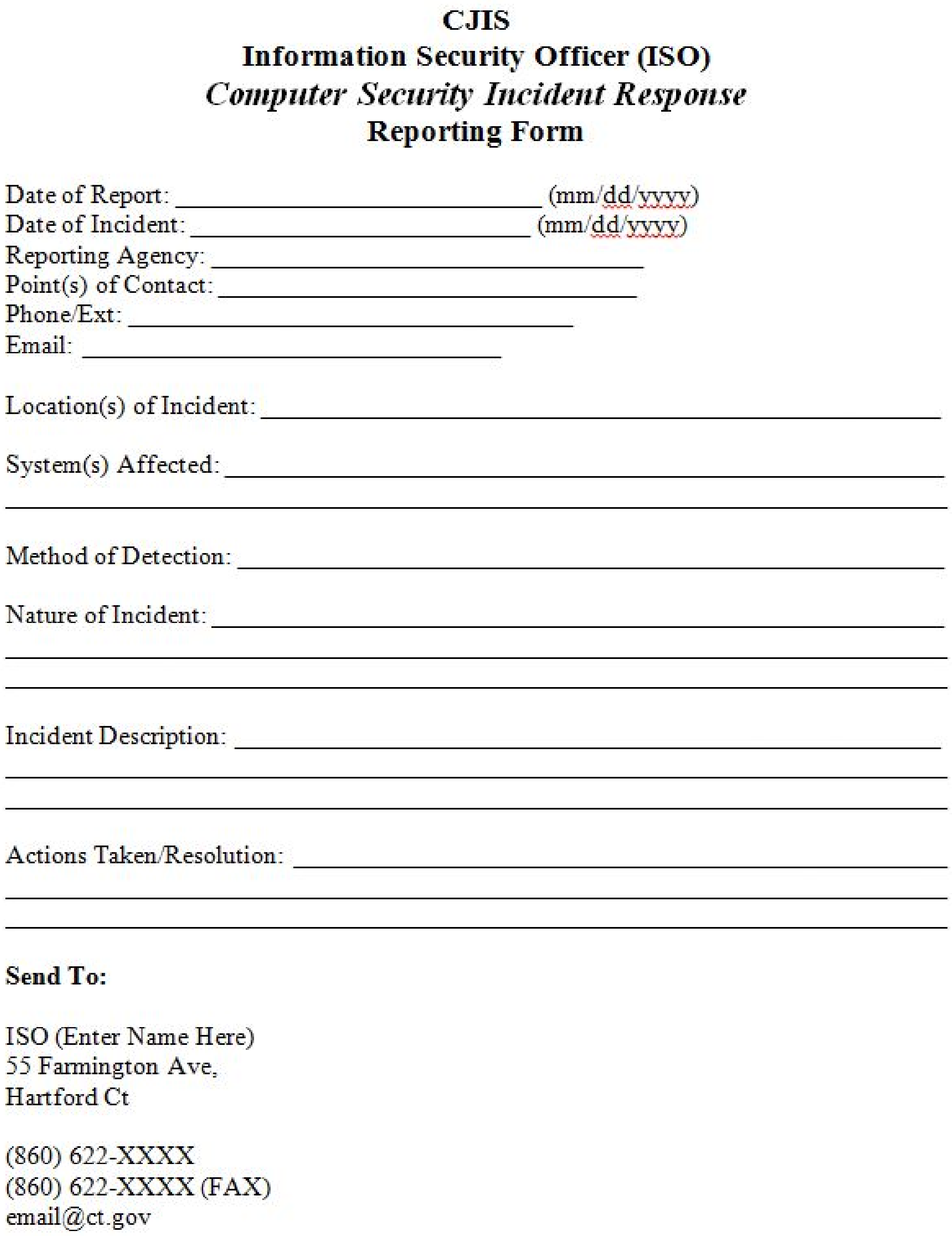
Print Name: ____

Relationship (Circle One): State Employee Vendor

CJIS Role: ____

Signature: ______________________________ **Date:** __________

Appendix IV. Sample Incident Notification Report



CJIS
Information Security Officer (ISO)
Computer Security Incident Response
Reporting Form

Date of Report: ____________________________ (mm/dd/yyyy)
Date of Incident: ___________________________ (mm/dd/yyyy)
Reporting Agency: __________________________________
Point(s) of Contact: ________________________________
Phone/Ext: ___________________________________
Email: _________________________________

Location(s) of Incident: ____

System(s) Affected: ____
____

Method of Detection: ____

Nature of Incident: ____
____
____

Incident Description: ____
____
____

Actions Taken/Resolution: ____
____
____

Send To:

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

(860) 622-XXXX
(860) 622-XXXX (FAX)
email@ct.gov

Appendix V. CT CJIS Security Compliance Assessment Form (CJIS-2)

The Connecticut Criminal Justice Information System Security Compliance Assessment Form (CJIS-2) is used as a mechanism for municipalities, State and Federal agencies to assess their compliance with the *CT CJIS Security Policy* as adopted by the State of Connecticut CJIS Governing Board. This form may be used as an internal document for an agency to assess their present level of compliance and subsequently perform necessary changes to attain compliance or submitted to the CJIS Support Group for assistance in attaining compliance.

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. Refer to CT CJIS Security Policy, sections 5.5.2.1, 5.5.2.2.**

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**

- **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:	

Appendix VI. CT CJIS Security Compliance Certification Form (CJIS-3)

The Connecticut Criminal Justice Information System Security Compliance Certification Form (CJIS-3) is used as a mechanism for municipalities, State and Federal agencies to certify their compliance with the *CT CJIS Security Policy* as adopted by the State of Connecticut CJIS Governing Board. This form must be submitted to the CJIS Support Group triennially on or before June 30th.

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 □ NO □**

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 □ NO □**
- **This firewall is configured to retain logs for a minimum of one (1) year.** **YES □ NO □**

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:	

Appendix VII. System Use Notification

The following guidelines pertain to system use:

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

Appendix VIII. Statues

6.13. Connecticut General Statute Sec. 54-142q

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 offender-based tracking system and information systems among criminal justice agencies.

(b) There shall be a Criminal Justice Information System Governing Board which shall be within the Office of Policy and Management 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 Public Safety, the Commissioner of Emergency Management and Homeland Security, 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 Chief information Officer of the Department of Information Technology, 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 co-chairpersons.

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 Office of Policy and Management 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: (l) 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 offender- based tracking 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 non-conviction 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 L. 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.)

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 infom1ation 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 Subsccs. (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 eff1cient 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 co-chairpersons and add chairpersons and ranking members of the judiciary committee as members of governing board. added new Subsec. (e) rehiring 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.

See Sec. 4-38ffor definition of"administrative purposes only".

Sec. 54-142r. Availability of data in offender-based tracking system. Procedures for obtaining data. (a) Any data in the offender-based tracking system, as defined in section 54-

142q, shall be available to the Chief Information Officer of the Department of lnformation Technology 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 deemed in subsection (b) of section 54-l42g, 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 Secretary of the Office of Policy and Management 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.)

History: P.A. 06-196 made technical changes, effective June 7. 2006.

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; and

(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; and

(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; and

(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; and

(7) Monitored and administered by the Criminal Justice Information Systems Governing Board, with the assistance of the Department of

Information Technology, provided major software and hardware needs may be provided and serviced by private, third-party vendors,

(g) Not later than July l, 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,

(Jan, Sp, Sess, P. A. 08-L S, 40.)

History: Jan, Sp, Sess, P.A. 08-1 effective January 25, 2008.

Appendix IX. Dictionary of Terms

AA

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions. Advanced Authentication is also called Multi-Factor or Two-Factor authentication.”

AC

An Agency Coordinator (AC) is a staff member of the CGA who manages the agreement between the contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

- Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
- Participate in related meetings and provide input and comments for system improvement.
- Receive information from the CGA (e.g., system updates) and disseminate it to appropriate contractor employees.
- Maintain and update manuals applicable to the effectuation of the agreement and provide them to the contractor.
- Maintain up-to-date records of contractor’s employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
- Train or ensure the training of contractor personnel. If contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
- The AC will not permit an untrained/untested or non-certified contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
- Where appropriate, ensure compliance by the contractor with NCIC validation requirements.
- Provide completed applicant fingerprint cards on each contractor employee who accesses the system to the CJA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the

system.

- Any other responsibility for the AC promulgated by the Executive Director.

ACL Access Control List (ACL) is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

CGA Contracting Government Agency (CGA) is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum.

CISO The CISO (chief information security officer) is a senior-level executive responsible for aligning security initiatives with enterprise programs and business objectives, ensuring that information assets and technologies are adequately protected.

CJA Criminal Justice Agencies (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.

CSO The Chief Security Officer (CSO) is the executive responsible for the organization's entire security posture, both physical and digital.

Degauss Degaussing is the process of decreasing or eliminating a remnant magnetic field. Degaussing is used to reduce magnetic fields in CRT monitors and to destroy data held on magnetic data storage.

Encryption Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. An encryption scheme usually uses a pseudo-random encryption key generated by an algorithm.

Everbridge Everbridge is an automated communication suite that sends out notifications when there is a disruption in service, whether it’s a natural disaster or an IT service outage.

FIPS 140-2 standard The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to accredit cryptographic modules. The title is Security Requirements for Cryptographic Modules. Initial publication was on May 25, 2001 and was last updated December 3, 2002. It is used to coordinate the requirements and standards for cryptography modules that include both hardware and software components.

HTTP The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

IPS A reactive system, also known as an intrusion prevention system (IPS), the IPS auto-responds to the suspicious activity by resetting the connection or by reprogramming the firewall to block network traffic from the suspected malicious source.

ISO The Information Security Officer (ISO) maintains the computer and information systems for an organization, under federal and state law regulations. This officer is responsible for introducing and implementing a company's technological resources and for the safety of an organization's computer-related technology.

Jailbreak Jailbreaking is the name given to the process used to modify the operating system running on an iPhone, iPod touch, or iPad to allow the user greater control over their device, including the ability to remove Apple-imposed restrictions and install apps obtained and other content through means other than the official App Store (among the most prevalent of these alternative sources is Cydia).

LASO Local Agency Security Officer is a security point of contact for local agencies that have access to criminal justice information.

MAC In the seven-layer OSI model of computer networking, media access control (MAC) data communication protocol is a sub layer of the data link layer, which itself is layer 2. The MAC sub layer provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g., Ethernet. The hardware that implements the MAC is referred to as a medium access controller.

MDM Mobile Device Management (MDM) is software that secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises. MDM functionality typically includes over-the-air distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, ruggedized mobile computers, mobile printers, mobile POS devices, etc.

NCJA Non-Criminal Justice Agency (NCJA) 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.

PII 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.

PKI A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

POC Point of Contact is a person or a department serving as the coordinator or focal point of information concerning an activity or program.

PSTN Public switched telephone network (PSTN) is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephony operators, providing infrastructure and services for public telecommunication. The PSTN consists of telephone lines, fiber optic cables, microwave transmission links, all interconnected by switching centers, thus allowing any telephone in the world to communicate with any other.

Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital in its core network and includes mobile and other networks, as well as fixed telephones.

SPAM Electronic spamming is the use of electronic messaging systems to send unsolicited bulk messages (spam), especially advertising, indiscriminately.

Spyware Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.

SSID Service set identifier (SSID) is a 1 to 32 byte string. This is normally a human-readable string and thus commonly called the "network name".

TAC Terminal Agency Coordinator (TAC) is the Point of Contact at an agency for matters relating to access to CT CJIS information.

TLS Transport layer security (TLS) is a cryptographic protocol designed to provide communication security over the Internet. It uses X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom they are communicating, and to exchange a symmetric key. This session key is then used to encrypt data flowing between the parties.

Trojan Horse A Trojan Horse is a generally non-self-replicating type of malware software program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm.

Virtualization Virtualization, in computing, refers to the act of creating a virtual (rather than actual) version of something, including but not limited to a virtual computer hardware platform, operating system (OS), storage device, or computer network resources.

VLAN Virtual local area network (VLAN) is a single layer-2 network that is partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them by one or more routers.

WEP Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in September 1999, its intention was to provide data confidentiality comparable to that of a traditional wired network. In 2003 the Wi-Fi Alliance announced that WEP had been superseded by Wi-Fi Protected Access (WPA). In 2004, with the ratification of the full 802.11i standard (i.e. WPA2), the IEEE declared that both WEP-40 and WEP-104 have been deprecated.

WLAN Wireless Local Area Network (WLAN) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider Internet. This gives users the ability to move around within a local coverage area and still be connected to the network.

WPA Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy).