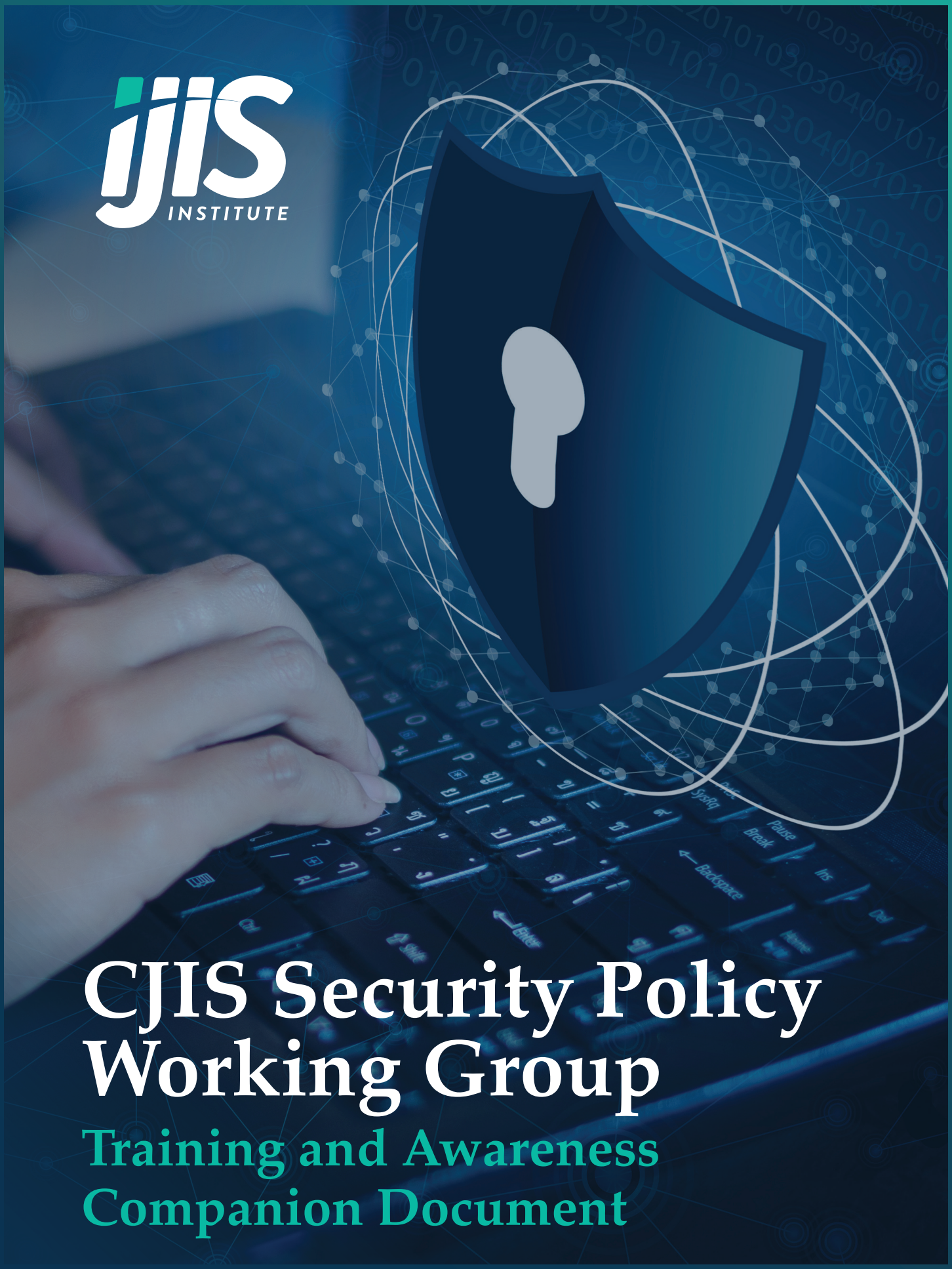


CJIS Security Policy Working Group

Training and Awareness Companion Document

Acknowledgements

This document is result of a collaboration between the IJIS Institute and the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division. The IJIS Institute is a nonprofit collaboration network that brings together innovative thinkers from the public and private sectors, national practice associations, and academic / research organizations working together to solve public sector mission, information sharing, policy and technology challenges.

IJIS Mission

To drive public sector technology innovation and empower information sharing to promote safer and healthier communities.

IJIS CJIS Security Policy Work Group Roster

Charlie Schaeffer, Chair	*Microsoft/Azure*
Jens Black	*Motorola Solutions*
Gerard Britton	*Enforsys Inc.*
Jeff Campbell	*FBI CJIS*
Ed Claughton	*PRI Management Group*
Monty Coats	*South Carolina Law Enforcement Division (SLED)*
Holden Cross	*FBI CJIS*
Brian DaSilva	*Mark43*
Matthew Doherty	*Sikich*
Jim Emerson	*NW3C*
Jason Emineth	*equivant*
Gerard Gallant	*Amazon Web Services*
Mike Lesko	*NEC*
Catherine Miller	*Montgomery County Maryland Police*
Maury Mitchell	*Alabama Law Enforcement Agency*
JC North	*Nlets*
Greg Park	*Livermore Police Department, CA*
Bill Philips	*Nlets*
Rob Serio	*Computer Projects of Illinois*
John Tomme	*Analysts*
George Vit	*South Brunswick, NJ Police Department*
Catherine Watson	*AT&T*
Chris Weatherly	*FBI CJIS*

Comments and Questions? They are always welcome! Please contact the IJIS Institute at **info@ijis.org** or **703-726-3697**.

Introduction

The CJIS Security Policy serves as a critical resource for criminal justice agencies by offering guidelines and best practices to protect the integrity, confidentiality, and availability of Criminal Justice Information (CJI). It provides rigorous security requirements, policies, and controls that must be implemented to maintain the trust and reliability of those maintaining and accessing this information. The CJIS Security Policy incorporates executive orders, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) recommendations, and nationally recognized guidance from the National Institute of Standards and Technology.

As technology and innovation continue to advance at an unprecedented pace, ensuring the security of sensitive information is paramount for entities storing and requesting access to CJI. With these critical needs in mind, the Federal Bureau of Investigation (FBI) continues to update the Criminal Justice Information Services (CJIS) Security Policy to provide a comprehensive framework for safeguarding data in an ever-changing environment.

Given the complex and constantly evolving policy requirements, it is imperative to have avenues to simplify and educate the stakeholder community, which includes but is not limited to criminal justice and law enforcement agencies, private sector service providers, nonprofit and academia organizations supporting the public sector community. The IJIS Institute, in partnership with the FBI CJIS Division, continues to collaborate in order to meet public sector mission goals.

Purpose of this Document

In support of and collaboration with the FBI's CJIS Division, the IJIS Institute constituted this Working Group to help address the complexity of the most recent updates to the CJIS Security Policy. Through collaboration of subject matter experts from public sector agencies, industry service providers, and supporting nonprofit organizations, these publications aim to provide template guidelines assisting agencies update their policies, procedures, and ultimately overall security measures. This publication specifically focuses on changes to the Awareness and Training sections of CJIS Security Policy version 5.9.2.

Policy and Procedures (AT-1)

New policy format and requirements based on NIST SP 800-53b.

NIST Policy Primer

As the CJIS Security Policy aligns with the NIST SP 800-53b Moderate baseline, the requirements for and format of agency security policies changes, and the emphasis on documenting procedures is heightened.

SP 800-53 groups related security controls into families such as System and Information Integrity (SI), Security Awareness and Training (AT), Media Protection (MP), and so on.

Each control in a family is numbered, and the first control in each family calls for a policy that specifies the implemented controls along with coverage of the purpose and scope of the policy, agency leadership's commitment to the policy, and the specific duties called for by the policy and what roles, groups, or personnel are responsible for them.

This section intends to give a quick introduction to writing NIST 800-53 compatible security policies and procedures. Core policy sections are in **bold**, and example text for the sections is in *italics*.

1. **Purpose**
    a. Things to consider:
        i. The "why" of the policy
        ii. Summarize the primary objective(s)
        iii. How does the policy fit with other agency policies, and/or into larger security/compliance efforts

    b. Guidance/Examples
        i. As part of a larger program to ensure compliance with the CJIS Security Policy, (AGENCY) must ensure that personnel with access to sensitive systems, data, or networks and the facilities that house them receive role-appropriate training prior to gaining access and on an annual basis thereafter.
        ii. To properly protect sensitive systems and data from losses due to the accidental or intentional misuse of information technology resources, personnel must be adequately trained in the principles of privacy and information security. The purpose of this document is to provide guidance on establishing and implementing a security awareness training program.

2. Scope

a. Things to consider:

i. To whom does the policy apply?

ii. Does the policy cover people, systems, devices, networks, or a combination?

iii. If the policy applies to personnel, are any personnel specifically exempted?

iv. Are there any external personnel (including contractors, consultants, service providers, partners, etc) with unescorted access to systems or facilities. In CSP, these personnel are generally covered by the policy if they have access to systems, networks, devices, or facilities.

b. Guidance/Examples

i. This policy applies to all (AGENCY) personnel, contractors, and any third parties with access to (AGENCY) facilities, systems, and/or networks.

3. Roles and Responsibilities

a. Things to consider:

i. In the agency, who is ultimately responsible for the security awareness and training program?

ii. Are they also responsible for the maintenance of training materials? If not, who is?

iii. Who delivers the training?

iv. Who maintains the records of training?

v. It is also generally advisable to note the team or position that is responsible for reviewing and updating the policy, along with the frequency of review (annual).

vi. In general, it is better to note a team or position that holds responsibility, rather than specific individuals (by name).

b. Guidance/Examples

i. RACI (Responsible, Accountable, Consulted, Informed) charts can be quite useful for documenting roles and responsibilities. (Information on RACI charts can be found at RACI Charts - How-to Guide and Templates)

ii. Example of a RACI chart:

	CJIS ISO	Human Resources	Training	Information Security Services	AGENCY Personnel	Frequency
Maintain records of Security Awareness Training for all AGENCY personnel, including the information security awareness letter	A	I		R		Annual
Conduct CJIS Security Awareness training for all AGENCY personnel	A	I	R	C		As Needed
Develop and maintain/review CJIS Security Awareness Training	A		R	C		Annual
Develop and maintain ongoing and supplementary Security Awareness Training	A		R	C		Monthly
Conduct ongoing and supplementary Security Awareness Training	A			R		Monthly
Participate in and successfully complete PII Awareness Training appropriate for role and access level (may be combined with CJIS Awareness training)	A				R	Annual
Participate in and successfully complete CJIS Security Awareness Training appropriate for role and access level	A				R	Annual
Participate in and successfully complete ongoing and supplementary Security Awareness Training	A				R	Monthly
Sign Security Awareness Training Acknowledgement Form	A	I	I		R	Annual
Distribute/display supplementary security awareness training materials (such as posters, handouts, etc)	A			R	I	Monthly

iii. A simple bulleted list of statements also works, such as:

- *The (AGENCY) Information Security Officer shall be responsible for creating and/or procuring the security awareness and training materials and reviewing them on an annual basis and as required by security events and/or assessment or audit findings.*
- *(AGENCY) Human Resources shall be responsible for maintaining current records of all security and awareness training activities and shall ensure that all personnel receive the required training for their role, both initially and on an annual basis.*

4. Management Commitment

a. Things to consider:

i. This statement can be stated as part of an overview, summary, or introduction to the policy

ii. Why is it important that the policy exist and be observed?

iii. Why is this function important to the agency?

b. Guidance/Examples

i. Information is a valuable (AGENCY) asset and must be protected from unauthorized disclosure, modification, or destruction. Initial and ongoing security awareness and training for (AGENCY) personnel is a vital component of an overall approach to the secure handling, storage, and processing of sensitive data and compliance with the CJIS Security Policy.

5. Controls and Requirements

a. This section can also be labeled as **Policy**.

b. Things to consider:

i. While it is generally acceptable for agencies to simply "copy and paste" the relevant section from CSP, the outcome of one or more agency leaders reviewing the CSP material through the lens of the agency's overall purpose and objectives tends to be a policy that is clearer to agency personnel and more easily integrated into agency operations.

ii. It is generally advisable to specify a technology that must be implemented over specifically dictating a given tool or solution (i.e. 'malicious code protection' as opposed to 'ACME Anti-Virus'). In general, a policy should advise/require specific outcomes (such as "malicious code protection" rather than anti-virus or specific technology recommendations) while procedures deal with specific products that might be in use.

iii. The policy itself represents the first control in the family, and as such does not need to be reflected IN the policy.

c. Guidance/Examples

i. Ensure that each control in the CSP section is referenced and restated as to how it is implemented at the agency.

ii. If the agency currently goes beyond the CSP requirements, or plans to, this should also be reflected in policy.

iii. *Reference any relevant timelines or required repetitions (training is required prior to granting access to CJI and must be repeated annually; training records must be maintained for three years to accommodate the triennial audit cycle).*

iv. *For Role-Based Training (AT-3), it is acceptable and may be helpful to group specific agency roles with their respective training levels, updating as roles are added or changed.*

v. *As the policy must be reviewed, at a minimum, on an annual basis, it is good to include a simple table at the end of the document that tracks the dates of review and changes, along with who made and/or approved the change.*

Procedure Primer

Along with the new policy requirements, the new CJISSECPOL version also places more emphasis on the need for procedures documenting how to perform tasks associated with implementation and management of implemented security controls.

1. Things to consider:
    a. Procedures should provide enough detail for a person with basic knowledge of the system or technology to carry out the task.
    b. Tasks performed by all personnel (such as accessing a security training application like CJISOnline) tend to benefit from screenshots, but policies targeted to roles such as system or network administrators or technical security staff generally won't require them.
    c. Document tools and access required, key points of contact if difficulty is encountered (this is especially helpful for procedures that would be used by all personnel), and the basic steps required to perform the task

2. Guidance/Examples
    a. The following is basic structure that can be used for procedures. It can be adopted as-is, but it is recommended to tailor it to suit the specific needs of the agency.
        i. Objective
            1. Summarize the task that the procedure documents
        ii. Tools and Access
            1. List any required tools, applications, websites, etc., and specify the required access level. It can be helpful to include contact information for the person/team that controls this access.
        iii. Procedure
            1. Give an overview of the steps required to complete the task.
            2. Procedures for tasks carried out by junior personnel and non-technical staff will generally need more detail than those intended for senior or technical staff.
        iv. Revision History
            1. As with the policy, keep a simple table at the end of the document.
            2. As with the policy, procedures may be reviewed in your audit.

Literacy Training and Awareness (AT-2)

Changes to the training requirements are critical for agency review and ultimately implementation. It is suggested that one or more of the following tools be utilized when delivering the training to your audiences.

Summary of changes

- Training must be completed PRIOR to granting CJI access (was within six months).
- Training must be repeated ANNUALLY (was biennial).
    - While initial training (prior to granting access) is ideally conducted over a short period of time, if not in one sitting, ongoing annual training can be conducted in periodic "batches" (such as monthly training) if all required topics are covered over the course of one year.
- New training topic required for persons with physical and/or logical access: Personally Identifiable Information.

Supplementary Training Materials (new)

One or more of:

1. Posters with security reminders placed around the secure area and/or workspace
    a. Posting signs and posters in prominent areas (restroom and break room doors, employee bulletin boards and other high traffic areas) is a good way to raise awareness around security topics such as malware, phishing, and other attacks that focus on end-users.
    b. Rotate materials every 4-6 weeks.
2. Supplies with security and privacy reminders provided to personnel
    a. This tends to work best in the early days of a new or revised security program, but over time the novelty tends to wear off.
3. Integration into logon screen messages
    a. Most users are used to breezing past the logon message, so while this one is an easy "check of the box", it may also be among the least effective.
4. Email advisories or other security information notices from organizational officials
    a. Periodic email advisories about vulnerabilities, remediation efforts, and similar can be a useful way to keep personnel apprised of security efforts and concerns.
5. Conducting awareness events (brown-bag sessions, webinars, briefings)
    a. Interactive live and online events with some degree of interactivity increase engagement and aid absorption of the topic.
    b. Some training providers, such as KnowBe4, offer short topic, interactive training exercises that can also be quite useful for increasing security awareness.

Tools and Technologies

As of January 2023, Peak Performance is in the process of updating the CJIS Security Awareness curriculum to reflect the new CJIS Security Policy requirements. There are also other service providers, such as KnowBe4, who offer CJIS-specific training, awareness materials (such as posters) as well as a broad range of security topics, both as focused training and as short, refresher activities that can serve as useful security awareness events, as mentioned above.

Role-Based Training (AT-3)

Summary of changes

- The levels of CJIS Security Awareness Training and their associated topics have been revised.

Level 1 Training

Personnel with unescorted physical access to agency facilities, but no access to systems or applications. This includes janitorial, cleaning, maintenance, and similar personnel, whether they are employed by the agency or a third party.

Level 1 Topics

1. Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties
2. Reporting Security Events
3. Incident Response Training
4. System Use Notification
5. Physical Access Authorizations
6. Physical Access Control
7. Monitoring Physical Access
8. Visitor Control
9. Personnel Sanctions

Level 2 Training

Personnel with non-administrative access to systems and applications that process or store CJI. Most agency users should receive Level 2 Training.

Level 1 Topics

1. Criminal Justice Information
2. Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information
3. Personally Identifiable Information
4. Information Handling
5. Media Storage
6. Media Access
7. Audit Monitoring, Analysis, and Reporting
8. Access Enforcement
9. Least Privilege
10. System Access Control
11. Access control Criteria

12. System Use Notification
13. Session Lock
14. Personally Owned Information Systems
15. Password security
16. Access Control for Display Medium
17. Encryption
18. Malicious Code Protection
19. Spam and Spyware Protection
20. Cellular Devices
21. Mobile Device Management
22. Wireless Device Risk Mitigations
23. Wireless Device Malicious Code Protection
24. Literacy Training and Awareness/Social Engineering and Mining
25. Identification and Authentication (Organizational Users)
26. Media Protection
27. Level 1 Topics

Level 3 Training

Personnel with administrative access to and/or security responsibilities for systems and/or applications that process CJI. System and network administrators and front-line information security personnel should receive Level 3 training.

Level 1 Topics

1. Access Control
2. System and Communications Protection and Information Integrity
3. Patch Management
4. Data backup and storage
5. Most recent changes to the CJIS Security Policy
6. Level 1 and 2 Topics

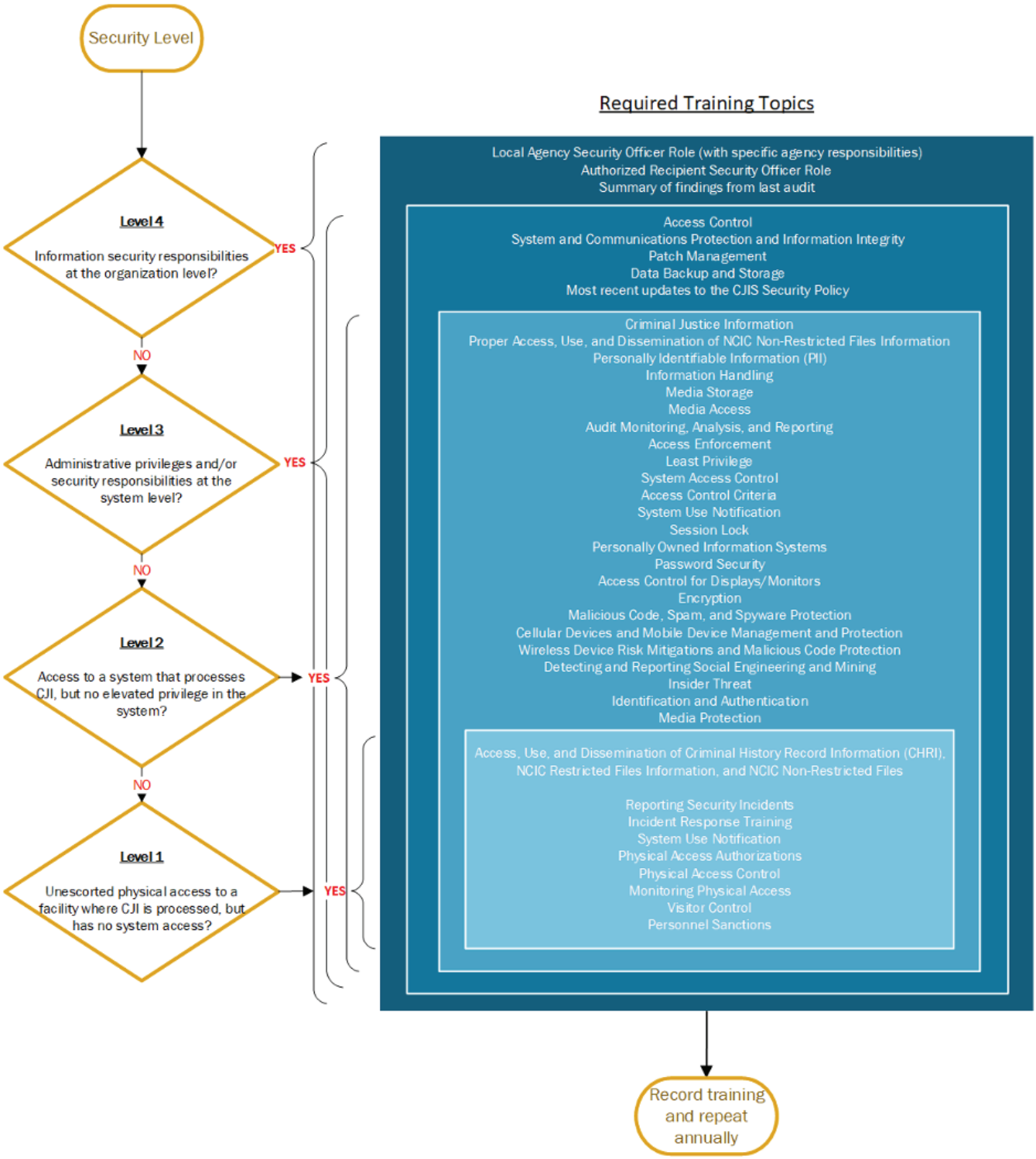
Level 4 Training

Personnel with organizational information security responsibilities. Agency Information Security Officers and other information security leaders should receive Level 4 Training.

Level 4 Topics

1. Local Agency Security Officer Role
2. Authorized Recipient Security Officer Role
3. Additional agency roles/responsibilities
4. Summary of audit findings from relevant previous audits (State, CSA, etc)
5. Level 1, 2, and 3 Topics

Training Topics by Level



Tools and Technologies

CJISOnline provides CJIS training solutions that are aligned to the CJISSECPOL requirements. Other training providers, notably KnowBe4, also offer compliant solutions for role-based training, as well as supplementary training materials (such as posters and short topic lessons on relevant topics such as phishing, social engineering, and malware.

Training Records (AT-4)

Summary of changes

- Training records must be kept for three years to accommodate the triennial audit cycle (the duration was not explicitly stated in previous versions)

AT-4 makes no other changes to requirements.

Tools and Technologies

CJISonline and KnowBe4 both maintain records of training and assessment results. For agencies that are using a different training source, it is possible to use tools like Smartsheet to build a simple schedule and tracker (that sends reminders to personnel when certifications are expiring) to manage security awareness training records.