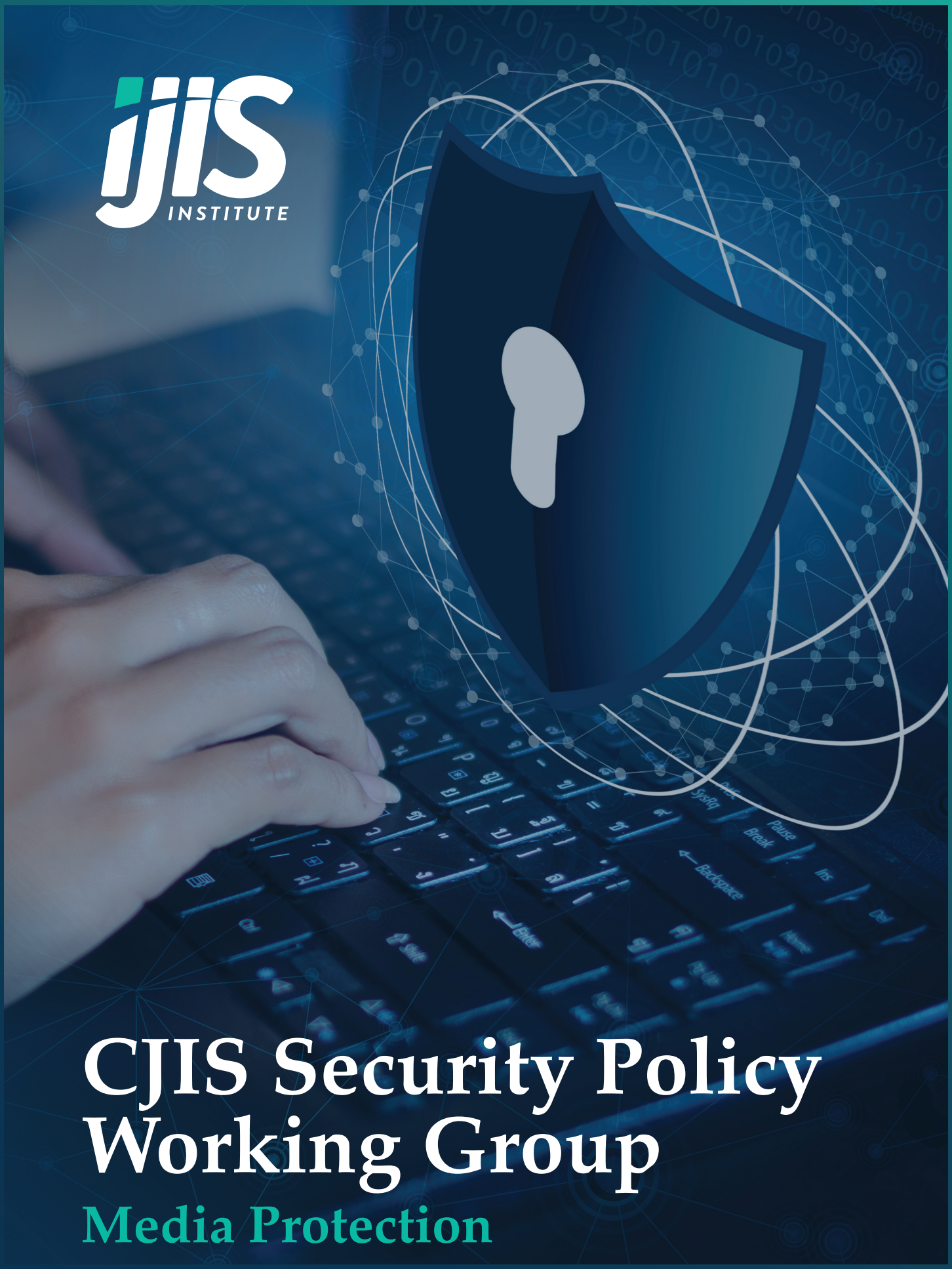

CJIS Security Policy Working Group

Media Protection

Acknowledgments

This document is result of a partnership 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	*Innova Solutions*
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.

CJIS_v5.9.2_Sec5.8_NIST800-53r5_MP

Summary of changes:

- Modernize the CJIS Security Policy requirements for:
  - Media Policy & Procedures,
  - Access
  - Marking
  - Storage,
  - Transport,
  - Sanitization
  - Use

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 policy 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), Identification and Authentication (IA), 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 document intends to give a quick introduction to writing NIST 800-53 compatible security policies and procedures. Core policy sections are in **bold**, and the 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. Develop, document, and disseminate to authorized individuals 1) Agency-level media protection policy and 2) Procedures to facilitate the implementation of the media protection policy.

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

b. Guidance/Examples

i. This policy applies to all authorized individuals.

3. Roles and Responsibilities

a. Things to consider:

i. In the agency, who is ultimately responsible for the specific security functions required by the policy?

ii. Who manages/maintains tools relevant to the effort?

iii. Who documents the effort?

iv. Who maintains records or performs periodic reviews of the policy and any documentation, procedures, or audit records/logs?

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

b. Guidance/Examples

i. *Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures;*

ii. *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)*

Example MP RACI of section MP:

	CJIS LASO	Human Resources	Training	Information Security Services	AGENCY Personnel	Frequency
Develop, document, and disseminate agency-level media protection policy.	A	C	I	R	I	Immediately
Develop, document, and disseminate procedures to facilitate the implementation of the media protection policy.	A	C	I	R	I	Immediately
Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures.	A	C	I	R	I	Immediately
Review and update media protection policy and procedures at least annually and following any security incidents.	A	C	I	R	I	At least Annually

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. Documented and implemented media protection policies and procedures ensure that access to digital and non-digital media in all forms is restricted to authorized individuals using authorized methods and processes.

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'). Generally, a policy should advise/require the use of a given technology, 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 before 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, annually, 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 emphasizes 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 all personnel would use), 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 agency's specific needs.
        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. Including contact information for the person/team that controls this access can be helpful.
        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.

MP-2 Media Access

Summary of changes:

- Media Access (MP-2) was separated from Media Storage (MP-4) while the media access control remains the same:
  - Restrict access to digital and non-digital media to authorized individuals.

MP-3 Media Marking

Summary of changes:

- Media Marking (MP-3) is a new control to mark all media – digital media is exempted from marking IF it remains in a CJIS-defined physically secure location or controlled area.
  - Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
  - Exempt digital and non-digital media containing CJI from marking if the media remain within physically secure locations or controlled areas.

MP-4 Media Storage

Summary of changes:

- Media Storage (MP-4) was separated from Media Access (MP-2) and has been modified to include a new control requiring the same media protections until destroyed.
  - Physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible; and
  - Protect system media types defined in MP-4 until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

MP-5 Media Transport

Summary of changes:

- Media Transport (MP-5) has been modified to now mandate that CJI transported outside a physically secure location be encrypted – there were previous encryption exceptions that have been removed:
  - Protect and control digital and non-digital media to help prevent data compromise during transport outside of the physically secure locations or controlled areas using encryption, as defined in Section 5.10.1.2 of this Policy. Physical media will be protected at the same level as the information would be protected in electronic form;
  - Restrict the activities associated with the transport of electronic and physical media to authorized personnel;
  - Maintain accountability for system media during transport outside of the physically secure location or controlled areas;
  - Document activities associated with the transport of system media and
  - Restrict the activities associated with transporting system media to authorized personnel.

MP-6 Media Sanitization

Summary of changes:

- Media Sanitization (MP-6) has been modified to combine the disposal of digital media and physical media into one control where it was previously two separate control statements. The previous requirement for agencies to ensure that the sanitization or destruction of digital media is witnessed or carried out by authorized personnel has been removed.
  - Sanitize or destroy digital and non-digital media before disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media before disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration, and
  - Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

MP-7 Media Use

Summary of changes:

- Media Use (MP-7) is a new control that is sanctionable as of October 1, 2023. The new control requires that digital and all digital media be "approved for use," and any digital media device is prohibited unless it has an identifiable owner. MP-7 now prohibits personally owned digital media devices such as diskettes, magnetic tapes, flash drives, compact discs, digital versatile discs, and removable hard disk drives.
    - Restrict the use of digital and non-digital media on agency-owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical, physical, or administrative controls and
    - Prohibit the use of personally owned digital media devices on all agency-owned or controlled systems that store, process, or transmit criminal justice information; and
    - Prohibit the use of digital media devices on all agency-owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner.