JEFF CAMPBELL

DEPUTY
INFORMATION
SECURITY OFFICER

FBI/CJIS DIVISION

CJIS SECURITY POLICY

2024 UTAH TAC CONFERENCE

SEPTEMBER 10, 2024

AGENDA

- CJIS Security Policy Modernization Update
- Why the CJIS Security Policy
- CJISSECPOL Priorities & Implementation
- Multi-Factor Authentication (MFA)
- FBI CJIS ISO Resources

CJIS SECURITY POLICY (CJISSECPOL) MODERNIZATION UPDATE

CJISSECPOL MODERNIZATION UPDATE

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

CJISSECPOL MODERNIZATION UPDATE

NIST SP800-53r5 Control Families (18 total)

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Assessment, Authorization, and Monitoring (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)
- Supply Chain Risk Management (SR)

CJISSECPOL MODERNIZATION UPDATE

CJIS Security Policy Roadmap

2021

Progress

Fall:

- *Brief: MP / IGTF*

2022

Progress

Spring:

- *Brief: IA / SA / AT*

Fall:

- *Publish v5.9.1*
- *Publish v5.9.2*
- *Brief: AC / IR / MA*

2023

Progress

Spring:

- *Brief: AU / CP / PE / PL / RA / SC*

Fall:

- *Publish v5.9.3*
- *Brief: CM*

2024

Anticipated

Spring:

- *Publish v5.9.4*
- *Brief: CA / PS / SA / SR*
- *Publish v5.9.5*

Fall:

- *Task Force(s)*

2025

Anticipated

Spring:

- *Publish v6.0*
- *Brief: Parking Lot Items*
- *Task Force*

Fall:

- *Brief: Topic Papers / Task Force Topics*

2026

Anticipated

Spring:

- *Publish v6.1*

Fall:

- *Brief: Topic Papers*


ANY
QUESTIONS?

WHY THE CJISSECPOL?

OVERVIEW OF CJIS SECURITY POLICY

Applies to everyone dealing with Criminal Justice Information (CJI)

- FBI/CJIS provided information

Shared Management Philosophy

- "The FBI said so…"

Information Security Requirements

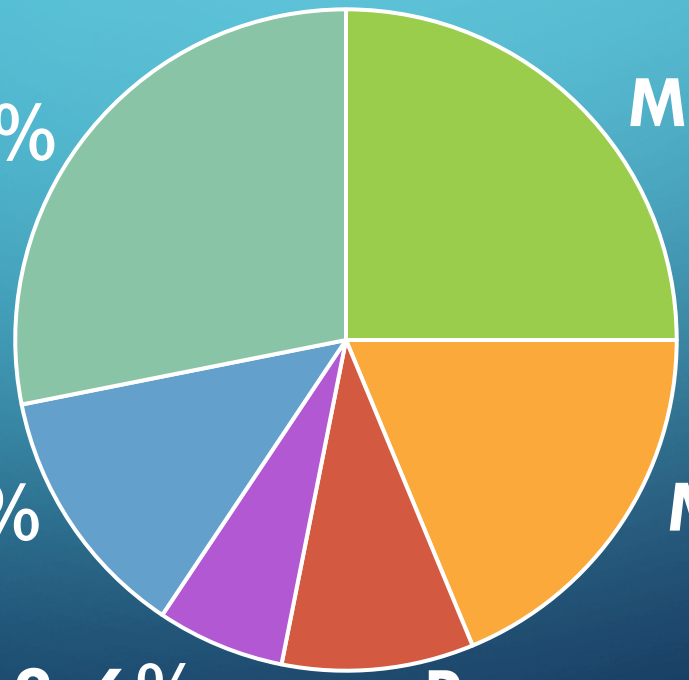
- Minimum set…but required for connectivity

Guidelines and Agreements

Trending Threats

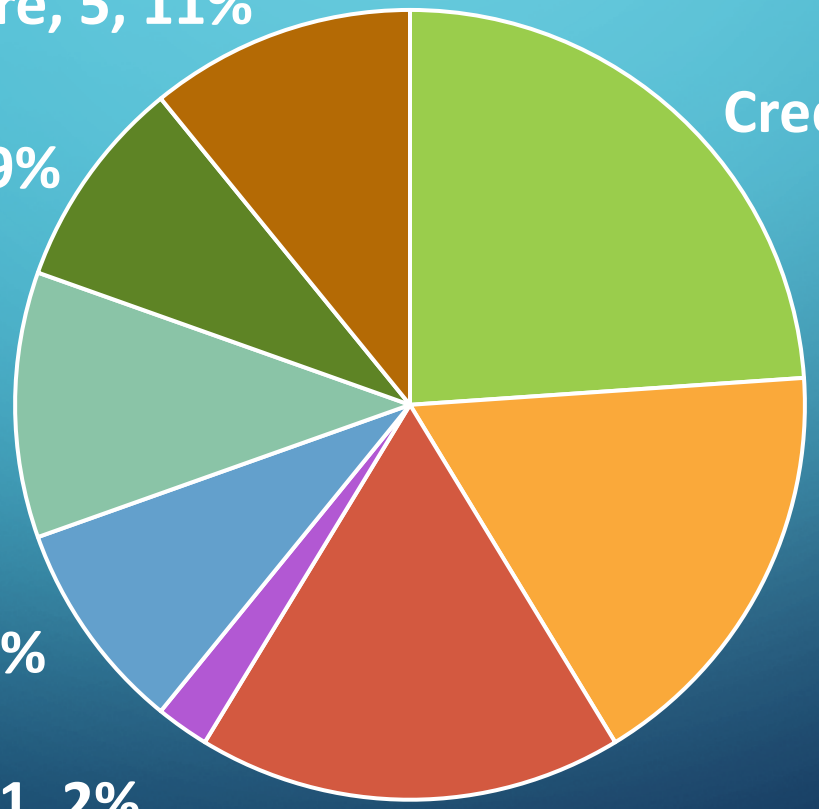
2021: 32 incidents reported to FBI CJIS ISO

Incidents



Trending Threats

2024 (to date): 46 incidents reported to FBI CJIS ISO



RECENT REPORTED INCIDENTS – CY24-Q1

Event Type	Other Info	Related Controls
Malware	Trojan Horse was discovered	SI-2; SI-3; SI-4; SC-7
Data Loss/Misuse	PC with CJI was discarded of improperly	MP-1; MP-5; MP-6; PE-16
Data Loss/Misuse	CJI was deleted by mistake and unrecoverable	MP-4; CP-9; CP-10
Ransomware	CAD/RMS system hit with Ransomware	SI-2; SI-3; SI-4; SC-7
Phishing	User clicked phishing email	AT-2; AT-3
Malware	CAD/RMS system was hit with malware and it spread to other systems causing an outage	SI-2; SI-3; SI-4; SC-7
Data Loss/Misuse	CJI left unattended	AT-2; AT-3; PE-3; MA-2
Data Loss/Misuse	Leaked information through email	AT-2; AT-3; SC-8; SC-13
Credential Compromise	User shared her account with access to CJI	AT-2; AT-3; AC-2
Malware	VPN suspected of containing malicious code	SI-2; SI-3; SI-4; SC-7
Malware	Domain Controller, GIS, and VOIP systems all affected by malware	SI-2; SI-3; SI-4; SC-7
Unauthorized Access	Somone was able to use a vulnerability to login to a system and start looking for data	SI-2; SI-3; SI-4; SC-7
Malware	Suspected Malware after port scans were being run on the network internally	SI-2; SI-3; SI-4; SC-7
Credential Compromise	Credentials with access to CJI were found online	AT-2; AT-3; IA-2
Unauthorized Disclosure	CJI was sent to someone who was not vetted properly	AT-2; AT-3
Data Loss/Misuse	Employee misused CJI data	AT-2; AT-3
Credential Compromise	Brute Force password attempts were being made	AC-7; IA-2
Unauthorized Access	Personnel obtained access to master key and was able to be in areas of CJI they were not supposed to be	PE-2; PE-3; PE-6

RECENT REPORTED INCIDENTS – CY24-Q2

Event Type	Other Info	Related Controls
Miscellaneous	Vulnerability discovered by external entity	SI-2; SI-4; RA-5; RA-7
Ransomware	Files were encrypted and held ransome	AT-2; AT-3; SI-2; SI-3; SI-4; SC-7
Malware	Domain Controller attacked	SI-2; SI-3; SI-4; SC-7
Credential Compromise	Users credentials were compromised	IA-2
Malware	VPN's hit with Zero-Day vulnerability	RA-5; SI-2; SI-3; SI-4; SC-7
Ransomware	Printers on their network were creating printouts letting them know their data had been stolen	AT-2; AT-3; SI-2; SI-3; SI-4; SC-7
Credential Compromise	Users account was compromised	IA-2
Unauthorized Disclosure	User provided CJI information to a person who had not yet been vetted properly.	AT-2; AT-3; AC-21
Unauthorized Access	Maintenance personnel were allowed into a room unescorted with CJI	MA-2; MA-5; PE-3; PE-8; PE-16
Malware	User downloaded malicious software	SI-2; SI-3; SI-4; SC-7
Credential Compromise	Credentials were compromised and accounts were access to view CJI	IA-2
Credential Compromise	Compromised VPN credentials led to Ransomware	IA-2
Unauthorized Access	Unauthorized maintenance personnel gained access to protected areas of CJI	MA-2; MA-5; PE-3; PE-8; PE-16
Unauthorized Disclosure	CHRI results were returned to the wrong agency	AT-2; AT-3
Data Loss/Misuse	PC with CJI was discarded of improperly	MP-1; MP-5; MP-6; PE-16
Unauthorized Disclosure	CJI Transmitted unencrypted	SC-8; SC-13
Ransomware	Brute force password attack leading to attempted ransomware	AC-7; IA-2
Phishing	Phishing attempt	AT-2; AT-3
Phishing	Phishing attempt	AT-2; AT-3
Phishing	Phishing attempt	AT-2; AT-3
Data Loss/Misuse	Laptop was stolen with CJI	PE-17
Ransomware	Ransomware attack on the Tribal Government Network	SI-2; SI-3; SI-4; SC-7
Unauthorized Disclosure	CJI was posted to Facebook	AT-2; AT-3; PL-4

RECENT REPORTED INCIDENTS – CY24-Q3

Event Type	Other Info	Related Controls
Credential Compromise	VPN Credentials compromised	IA-2
Data Loss/Misuse	Laptop was stolen with CJI	PE-17
Credential Compromise	Email was compromised	IA-2
Credential Compromise	Email was compromised	IA-2
Credential Compromise	Email was compromised	IA-2

CJIS SECURITY POLICY PRIORITIES & IMPLEMENTATION

CJIS APB: CONTROL PRIORITIES & IMPLEMENTATION

- The Process:
  - Three-step solution:
    - Identify a subset of controls for immediate implementation to significantly reduce risk
    - Allow a zero-cycle audit for remaining controls
    - Create priority tiering matrix to assist in implementation during the zero-cycle audit

CJIS APB: CONTROL PRIORITIES & IMPLEMENTATION

- The Process:
  - Step 1: Controls for immediate implementation
    - Priority Code 1 [P1] controls identified by cross-mapping the NIST 800-53r5.1 "moderate baseline" security controls to MITRE ATT&CK® data
    - Cross-mapping paired the number of attacks with each associated individual control
    - EXAMPLE: MITRE listed 332 attacks associated with SI-4 Information System Monitoring.
    - An average risk score was developed by dividing the total attacks by the total number of affected moderate controls

$$\frac{4{,}367}{81} = 54$$

    - Results in 73 controls and control enhancements scoring above the average

CJIS APB: CONTROL PRIORITIES & IMPLEMENTATION

- The Process:
  - Step 2: Allow a zero-cycle audit for remaining controls
    - Zero-cycle audit for all modernized controls which are not existing (i.e., part of v5.9) and not identified as being [P1]
    - Roughly 56% of all controls
    - Auditable and sanctionable after the zero-cycle audit period has ended
    - Zero-cycle timeframe 1 OCT 2024 – 30 SEP 2027

CJIS APB: CONTROL PRIORITIES & IMPLEMENTATION

- The Process:
  - Step 3: Create priority tiering matrix to assist in implementation during the zero-cycle audit
    - Remaining non-[P1] controls assigned additional prioritization codes:
      - Priority Code 2 [P2]
      - Priority Code 3 [P3]
      - Priority Code 4 [P4]
    - Priorities assist in making sequencing decisions for implementation
      - Priority Code 2 [P2] implemented after [P1] and before [P3] & [P4]
      - Priority Code 3 [P3] implemented after [P2] and before [P4]
      - Priority Code 4 [P4] implemented after [P3]
    - Ensures implementation is accomplished in a manner of dependency
    - Implementation does not imply any defined level of risk mitigation until all controls have been implemented.

CJIS APB: CONTROL PRIORITIES & IMPLEMENTATION

- Markings (from CJISSECPOL Section 1.4):

Effective in version *5.9.5*, priority and implementation markings have been added to the modernized controls. Based on the FBI Director approved APB recommendation, beginning October 1, 2024, requirements existing prior to the CJISSECPOL modernization (i.e., version 5.9) and those identified as Priority 1 ([Priority 1]) will be the set of sanctionable requirements.

- Non-modernized sections do not have markings but are considered "existing" requirements and continue to be auditable and sanctionable.
- "Existing" modernized requirements and indicated by the [Existing] marking.
- Priority 1 modernized requirements are indicated by the [Priority 1] marking.
- All [Priority 2], [Priority 3], and [Priority 4] modernized requirements fall into a zero-cycle status. The zero-cycle begins October 1, 2024 and ends September 30, 2027.

CJIS APB: CONTROL PRIORITIES & IMPLEMENTATION

- Requirements Companion Document (RCD)

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-15: System and Information Integrity (SI)								
		POLICY AND PROCEDURES	a. Develop, document, and disseminate to all organizational personnel with system and information integrity responsibilities and information system owners:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Agency-level system and information integrity policy that:	Zero-cycle	P2	Agency	Agency	Agency
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	Agency	Agency	Agency
			ent with applicable laws, executive orders, directives, regulations, ards, and guidelines; and	Zero-cycle	P2	Agency	Agency	Agency
			es to facilitate the implementation of the system and informatio and the associated system and information integrity controls;	Zero-cycle	P2	Agency	Agency	Agency
			e organizational personnel with system and information integrity to manage the development, documentation, and dissemination of information integrity policy and procedures; and	Zero-cycle	P2	Agency	Agency	Agency
			and update the current system and information integrity:	Zero-cycle	P2	Agency	Agency	Agency
			nually and following any security incidents involving unauthorized r systems used to process, store, or transmit CJI; and	Zero-cycle	P2	Agency	Agency	Agency
			es annually and following any security incidents involving cess to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	Agency	Agency	Agency
			eport, and correct system flaws;	Existing	P1	Both	Service Provider	Service Provider
			ware and firmware updates related to flaw remediation for nd potential side effects before installation;	10/1/2024	P1	Both	Service Provider	Service Provider
			curity-relevant software and firmware updates within the number of	Existing	P1	Both	Service Provider	Service Provider
				10/1/2024	P1	Both	Service Provider	Service Provider
				10/1/2024	P1	Both	Service Provider	Service Provider
				10/1/2024	P1	Both	Service Provider	Service Provider
				10/1/2024	P1	Both	Service Provider	Service Provider
			organizational configuration	10/1/2024	P1	Both	Service Provider	Service Provider
			licable security-relevant software and ty scanning tools as least quarterly or JI or systems used to process, store, or	10/1/2024	P1	Both	Service Provider	Service Provider
			code protection mechanisms at system e malicious code;	10/1/2024	P1	Both	Service Provider	Service Provider
			protection mechanisms as new releases onal configuration management policy	Existing	P1	Both	Service Provider	Service Provider
			mechanisms to:	Existing	P1			
		"	1. Perform periodic scans of the system at least daily and real-time scans of files from external sources at network entry and exit points and on all servers and endpoint devices as the files are downloaded, opened, or executed in accordance with organizational policy; and	Existing	P1	Both	Service Provider	Service Provider

- CJISSECPOL

AU-3 CONTENT OF AUDIT RECORDS

[Existing] [Priority 2]

Control:

Ensure that audit records contain information that establishes the following:

(3) CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

[Priority 2]

Control:

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).

CJIS APB: CONTROL PRIORITIES & IMPLEMENTATION

- Priority 1 [P1] Controls (22):

No.	Control Name	Enhancements	Priority
AC-2	ACCOUNT MANAGEMENT	AC-2 (1) (2) (3) (4) (5) (13)	P1
AC-3	ACCESS ENFORCEMENT	AC-3 (14)	P1
AC-4	INFORMATION FLOW ENFORCEMENT	AC-4	P1
AC-5	SEPARATION OF DUTIES	AC-5	P1
AC-6	LEAST PRIVILEGE	AC-6 (1) (2) (5) (7) (9) (10)	P1
AC-17	REMOTE ACCESS	AC-17 (1) (2) (3) (4)	P1
AC-20	USE OF EXTERNAL SYSTEMS	AC-20 (1) (2)	P1
CA-7	CONTINUOUS MONITORING	CA-7 (1) (4)	P1
CM-2	BASELINE CONFIGURATION	CM-2 (2) (3) (7)	P1
CM-5	ACCESS RESTRICTIONS FOR CHANGE	CM-5	P1
CM-6	CONFIGURATION SETTINGS	CM-6	P1
CM-7	LEAST FUNCTIONALITY	CM-7 (1) (2) (5)	P1
CM-8	SYSTEM COMPONENT INVENTORY	CM-8 (1) (3)	P1
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	IA-2 (1) (2) (8) (12)	P1
IA-5	AUTHENTICATOR MANAGEMENT	IA-5 (1) (2) (6)	P1
RA-5	VULNERABILITY MONITORING AND SCANNING	RA-5 (2) (5) (11)	P1
SC-7	BOUNDARY PROTECTION	SC-7 (3) (4) (5) (7) (8) (24)	P1
SI-2	FLAW REMEDIATION	SI-2 (2)	P1
SI-3	MALICIOUS CODE PROTECTION	SI-3	P1
SI-4	SYSTEM MONITORING	SI-4 (2) (4) (5)	P1
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	SI-7 (1) (7)	P1
SI-10	INFORMATION INPUT VALIDATION	SI-10	P1

CJIS APB: CONTROL PRIORITIES & IMPLEMENTATION

- Remaining Controls:
  - Priority Two, Three and Four controls
    - Implemented during “Zero Cycle” period
      - Noncompliance noted, but not sanctioned by CJIS APB
    - Must be implemented by October 1, 2027

CJIS APB: CONTROL PRIORITIES & IMPLEMENTATION

- Priority 2 [P2] Controls (107):

Enhancements	Enhancements	Enhancements	Enhancements	Enhancements
AC-1	CM-9	MA-1	PS-1	SC-5
AC-8	CM-11	MP-1	PS-2	SC-8 (1)
AC-18 (1) (3)	CM-12 (1)	MP-2	PS-3	SC-12
AC-19 (5)	CP-1	MP-4	PS-4	SC-13
AT-1	CP-2 (1) (3) (8)	MP-5	PS-7	SC-15
AT-2 (2) (3)	CP-6 (1) (3)	MP-6	RA-1	SC-17
AT-3	CP-7 (1) (2) (3)	MP-7	RA-2	SC-20
AT-3 (5)	CP-8 (1) (2)	PE-1	RA-3 (1)	SC-21
AU-1	CP-9 (1) (8)	PE-2	RA-7	SC-22
AU-2	CP-10 (2)	PE-3	RA-9	SC-23
AU-3 (1)	IA-1	PE-4	SA-1	SC-28 (1)
AU-3 (3)	IA-3	PE-6 (1)	SA-2	SC-39
AU-4	IA-4 (4)	PE-9	SA-3	SI-1
AU-5	IA-7	PE-10	SA-4 (1) (2) (9) (10)	SI-5
AU-6 (1) (3)	IA-8 (1) (2) (4)	PE-11	SA-8 (33)	SI-16
AU-8	IA-11	PE-12	SA-9 (2)	SR-1
AU-9 (4)	IA-12 (2) (3) (5)	PE-13 (1)	SA-10	SR-5
AU-12	IR-1	PE-14	SA-11	SR-6
CA-1	IR-4 (1)	PE-15	SA-22	SR-11 (1) (2)
CA-3	IR-5	PL-1	SC-1	
CM-1	IR-6 (1) (3)	PL-2	SC-2	
CM-3 (2) (4)	IR-8 (1)	PL-8	SC-4	

CJIS APB: CONTROL PRIORITIES & IMPLEMENTATION

- Priority 3 [P3] Controls (40):

Enhancements	Enhancements
AC-7	PE-16
AC-12	PE-17
AC-21	PL-4 (1)
AU-7 (1)	PL-10
CA-2 (1)	PL-11
CA-6	PS-5
CA-9	SA-5
CM-4 (2)	SA-15 (3)
CM-10	SC-10
CP-3	SC-18
CP-4 (1)	SI-8 (2)
IA-6	SI-11
IR-2	SI-12 (1) (2) (3)
IR-2 (3)	SR-2 (1)
IR-3 (2)	SR-3
IR-7 (1)	SR-8
MA-2	SR-10
MA-4	SR-12
MA-5	
MA-6	
MP-3	
PE-5	

- Priority 4 [P4] Controls (14):

Enhancements
AC-11 (1)
AC-14
AC-22
AT-4
AU-11
CA-5
MA-3 (1) (2) (3)
PE-8 (3)
PL-9
PS-6
PS-8
PS-9
SI-18 (4)
SI-19

MULTI-FACTOR AUTHENTICATION (MFA)

IDENTIFICATION AND AUTHENTICATION (IA)

- IA-2: IA (ORGANIZATIONAL USERS)
  - Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.
- *IA-2(1): Implement multi-factor authentication for access to privileged accounts.*
- *IA-2(2): Implement multi-factor authentication for access to non-privileged accounts.*

October 1, 2024

IDENTIFICATION AND AUTHENTICATION (IA)

- IA-5: AUTHENTICATOR MANAGEMENT
  - *Authentication Assurance Level (AAL) 2*
    - *CJI = MODERATE*
  - *Authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators*
    - **Unless multi-factor authenticator; use Memorized Secret plus…*
    - **Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (something you have).*
    - **Device unlock is NOT a factor of authentication*

October 1, 2024

IDENTIFICATION AND AUTHENTICATION (IA)

- IA-5: AUTHENTICATOR MANAGEMENT | AUTHENTICATOR TYPES
  - *Authenticator Types*
    - Memorized Secret (PW/PIN)
    - Look Up Secrets
    - *Out of Band*
    - One Time Passcode
    - *Cryptographic Authenticators*
      - *Software based*
      - *Hardware based*

October 1, 2024

IDENTIFICATION AND AUTHENTICATION (IA)

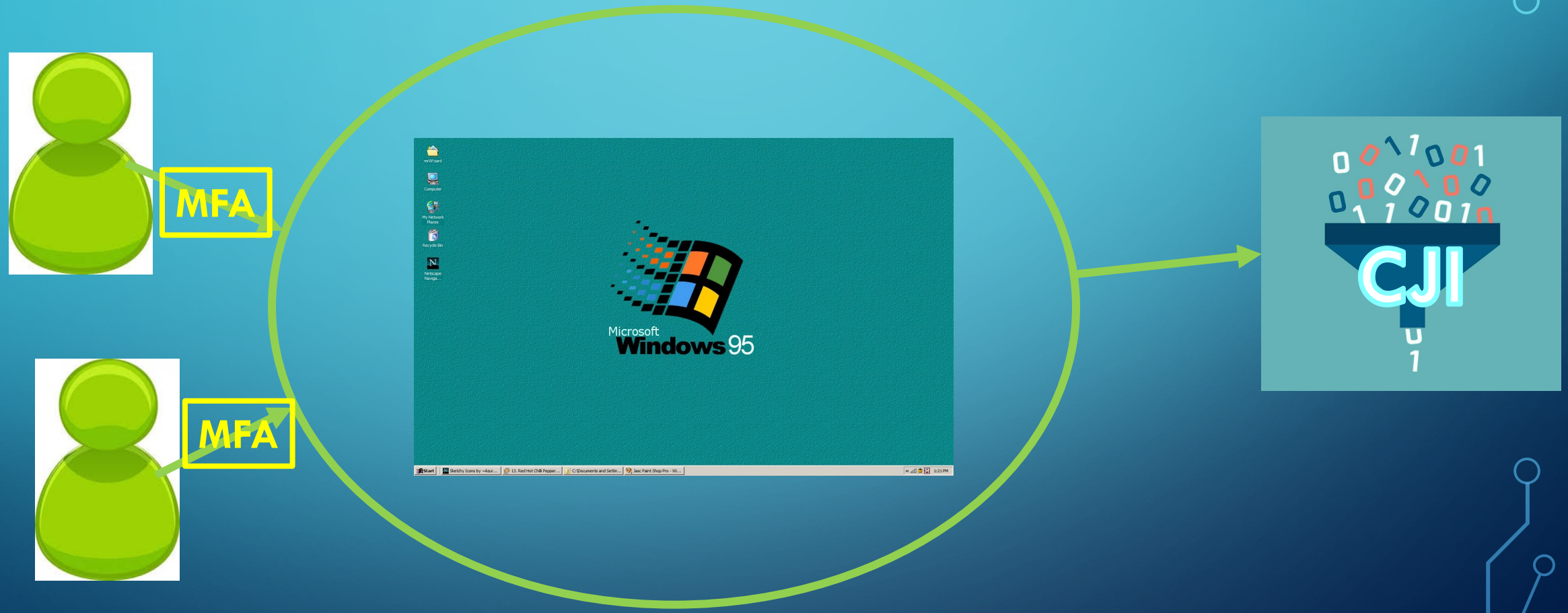
- IA-5: AUTHENTICATOR MANAGEMENT cont'd

KEY THING TO REMEMBER:

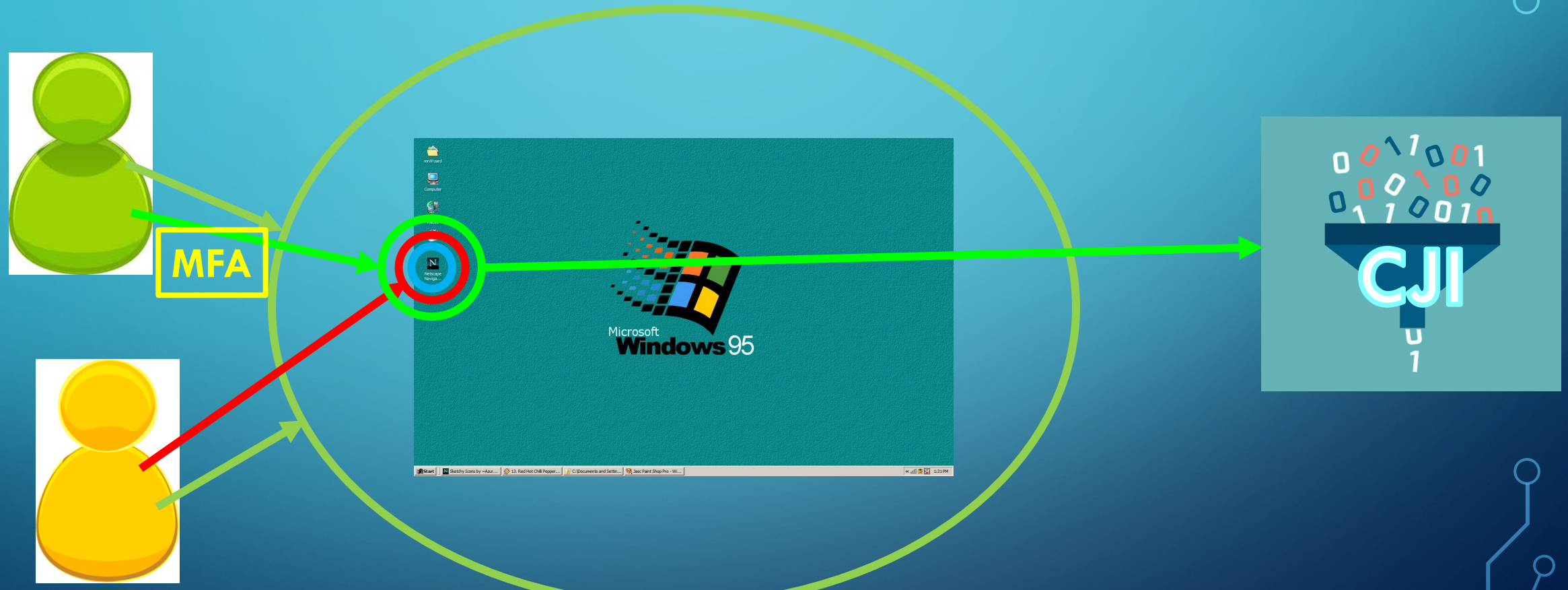
REQUIREMENTS IN IA-5(1) 'a' THRU 'J' AND ONLY THE ONES FOR THE AUTHENTICATOR(S) YOU HAVE IMPLEMENTED ARE REQUIRED TO BE MET

MFA USE CASES

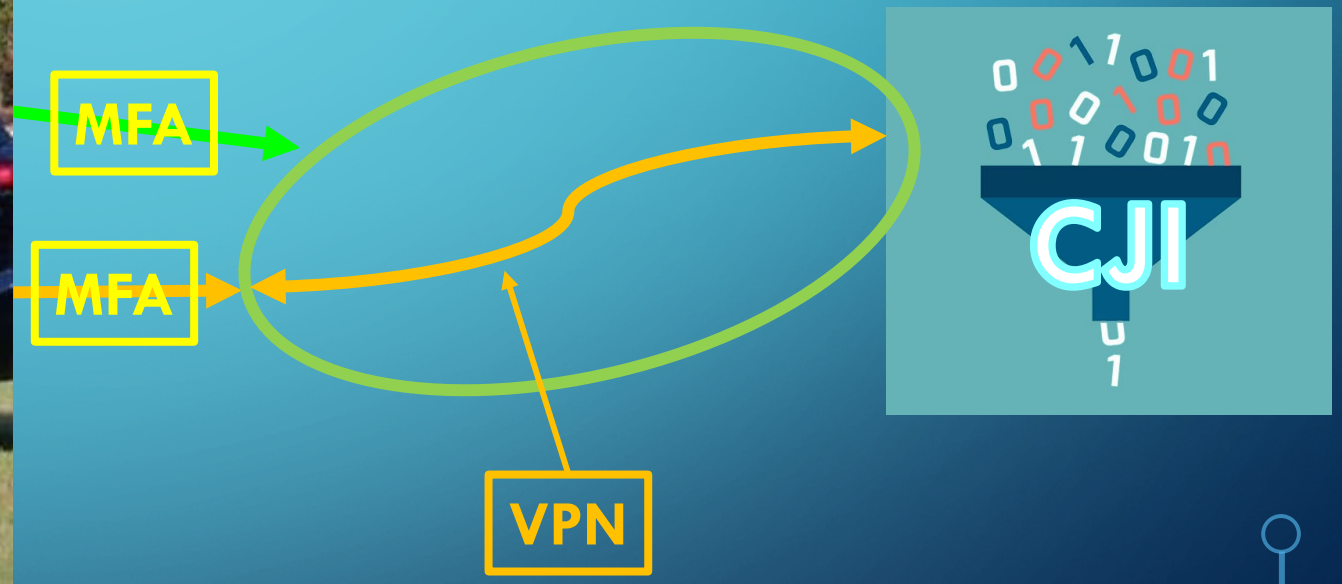
MFA USE CASE #1: ALL USERS, ACCESS ALL RESOURCES



MFA USE CASE #2: SOME USERS ACCESS CJI RESOURCES



MFA USE CASE #3: ALL MDT USERS, ACCESS ALL RESOURCES



FBI CJIS ISO RESOURCES

CJIS ISO Program

- Steward the CJIS Security Policy for the Advisory Policy Board
  - Draft and present topic papers at the APB meetings
- Provide Policy support to state ISOs and CSOs
  - Policy Clarification
  - Solution technical analysis for compliance with the Policy
  - Operate a public facing web site on FBI.gov: CJIS Security Policy Resource Center
- Provide training support to ISOs
- Provide policy clarification to vendors in coordination with ISOs
- IJIS / IACP Podcasts

iso@fbi.gov

CJISSECPOL Resource Center Website

CJIS Security Policy Resource Center

Home | Requirements Companion Document (PDF | Excel) | 2024 ISO Symposium Presentations | Use Cases | Links of Importance | Submit a Question

Download Criminal Justice Information Services (CJIS) Security Policy - Version 5.9.5

DOCUMENT | PAGES | TEXT | Zoom | Search

U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

Version 5.9.5
07/09/2024

Page 1 of 451

Requirements Companion document

- Companion document to the CJIS Security Policy
- Lists every requirement & “shall” statement, and corresponding location
- Lists the “Audit / Sanction” date for each requirement (modernization)
- Lists the control “Priority”
- Cloud “matrix” which shows the technical capability to meet requirements
- Updated annually in conjunction with the CJIS Security Policy
- New Excel version available

iso@fbi.gov

Requirements Companion document

Ver 5.9.4 Location and New Requirement	Ver 5.9.5 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Priority	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
CJIS Security Policy Section 5-15: System and Information Integrity (SI)								
5.15: SI-1	5.15: SI-1	POLICY AND PROCEDURES	a. Develop, document, and disseminate to all organizational personnel with system and information integrity responsibilities and information system owners:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Agency-level system and information integrity policy that:	Zero-cycle	P2	Agency	Agency	Agency
		"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Zero-cycle	P2	Agency	Agency	Agency
		"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Zero-cycle	P2	Agency	Agency	Agency
		"	2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;	Zero-cycle	P2	Agency	Agency	Agency
		"	b. Designate organizational personnel with system and information integrity responsibilities to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and	Zero-cycle	P2	Agency	Agency	Agency
		"	c. Review and update the current system and information integrity:	Zero-cycle	P2	Agency	Agency	Agency
		"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Zero-cycle	P2	Agency	Agency	Agency
		"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Zero-cycle	P2	Agency	Agency	Agency
5.15: SI-2	5.15: SI-2	FLAW REMEDIATION	a. Identify, report, and correct system flaws;	Existing	P1	Both	Service Provider	Service Provider
		"	b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	c. Install security-relevant software and firmware updates within the number of days listed after the release of the updates;	Existing	P1	Both	Service Provider	Service Provider
		"	• Critical – 15 days	10/1/2024	P1	Both	Service Provider	Service Provider
		"	• High – 30 days	10/1/2024	P1	Both	Service Provider	Service Provider
		"	• Medium – 60 days	10/1/2024	P1	Both	Service Provider	Service Provider
		"	• Low – 90 days; and	10/1/2024	P1	Both	Service Provider	Service Provider
		"	d. Incorporate flaw remediation into the organizational configuration management process.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-2 (2)	5.15: SI-2 (2)	(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS	Determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools as least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI.	10/1/2024	P1	Both	Service Provider	Service Provider
5.15: SI-3	5.15: SI-3	MALICIOUS CODE PROTECTION	a. Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;	10/1/2024	P1	Both	Service Provider	Service Provider
		"	b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;	Existing	P1	Both	Service Provider	Service Provider
		"	c. Configure malicious code protection mechanisms to:	Existing	P1			
		"	1. Perform periodic scans of the system at least daily and real-time scans of files from external sources at network entry and exit points and on all servers and endpoint devices as the files are downloaded, opened, or executed in accordance with organizational policy; and	Existing	P1	Both	Service Provider	Service Provider

FBI CJIS ISO Contact Information

Chris Weatherly
FBI CJIS ISO

Jeff Campbell
FBI CJIS Deputy ISO

Holden Cross
Sr. Technical Analyst

iso@fbi.gov