COLORADO
9-1-1 PROGRAM

New CJIS Security Requirements

Are You Ready?

Oct. 8, 2026

SECULORE®
a Motorola Solutions Company

SecuLore/Motorola Solutions
Colorado Cybersecurity Team



Frank Arico
SecuLore/Motorola Solutions

Sales and Strategic Channel Manager
➢Member of the APCO International Cybersecurity Committee
847.875.2400 mobile #
frank.arico@motorolasolutions.com



Angie Wineland
Motorola Solutions
Cybersecurity Sales Account Executive
720.935.6198 mobile #
angie.wineland@motorolasolutions.com

Need for Change
and
Security Enhancements

Financial Impacts for the Public Sector



The average cost of a data breach in the public sector, which includes law enforcement and other government agencies, was **$2.86 million** in 2025



This is lower than the global average (**$4.45 million**), but the impact on public trust and operations can be more significant

Impact of Cyber Threats

- Personal Data Exposure
- Value to Threat Actors
- Dangerous Disruptions
- Impact on Investigations
- Public Safety and Trust



Lack of Established Processes



- Center for Internet Security (CIS) 2025 cybersecurity review found that the biggest weaknesses in state/local government's cybersecurity program is that those programs are still being developed
- Various response activities (including incident response plans) may be in place, however are outdated and not formalized or tested
- Other issues found
  - Insufficient funding
  - Increased sophistication of attacks
  - Lack of documented process
  - Limited access to cybersecurity processionals
  - Same concerns have been cited **for at least eight years, according to the report**

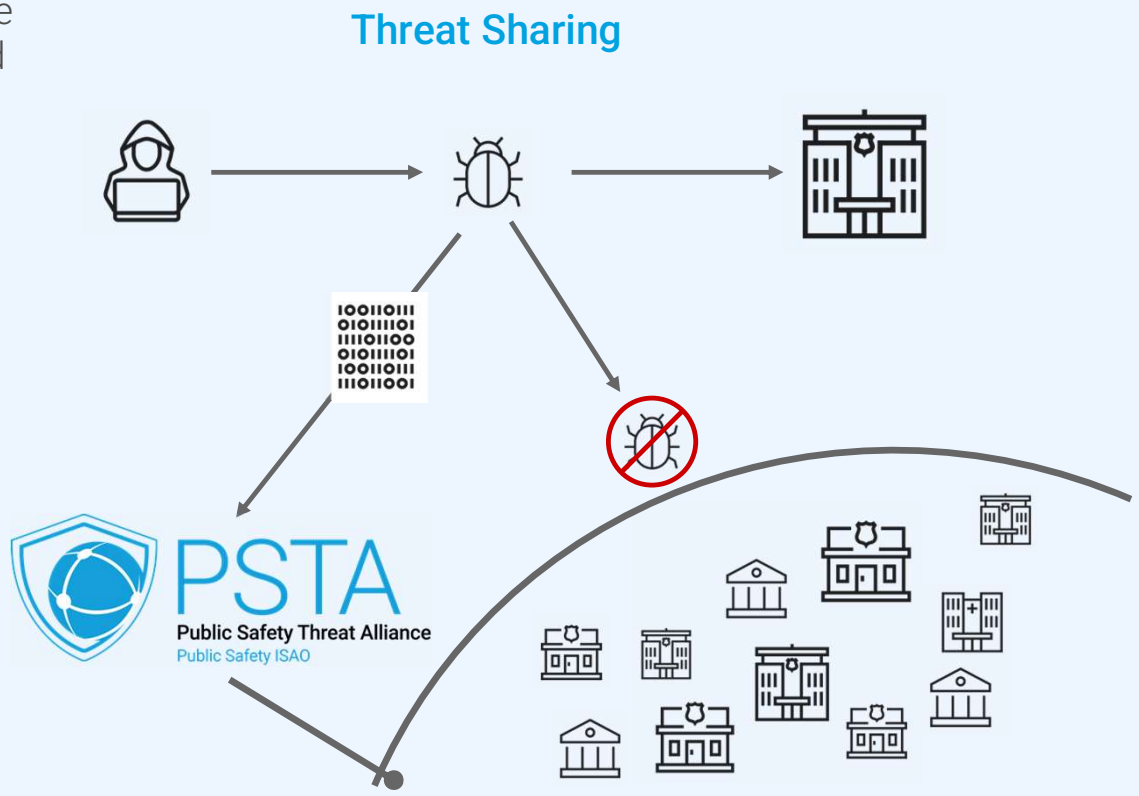
Public Safety Threat Alliance

Information sharing and analysis organization (ISAO)

Membership in the Public Safety Threat Alliance (PSTA) is open to all public safety agencies and partners at no cost

- Secure Portal for Information Sharing
- Finished Intelligence Reports
  - Joint reports: MS-ISAC & APCO
- Vulnerability & Threat Advisories
- TTXs (Tabletop Exercises)
- Dark Web Insights & Monitoring
- Quarterly Webinars
- Monthly Analyst Calls
- Automated Threat Feed

PSTA Sign up



Key CJIS Changes

CJIS Security Policy v6.0

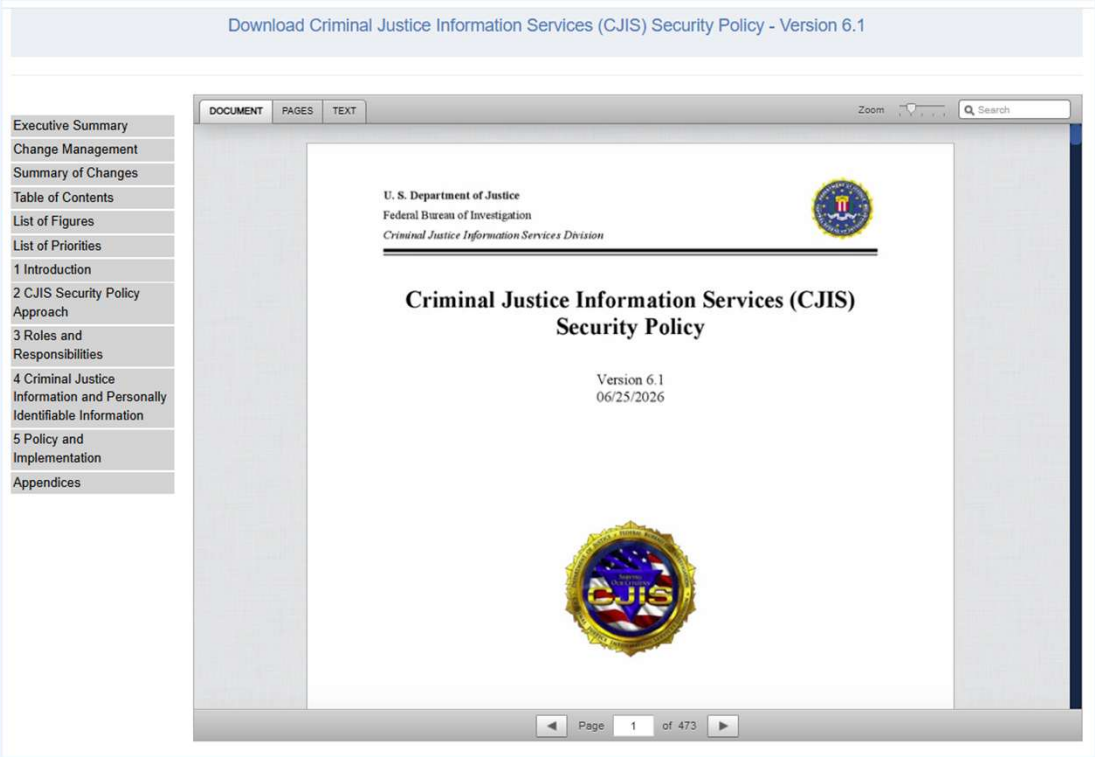
Changes released 12/27/2024

- ☑ Assessment, Authorization & Monitoring
- ☑ Personnel Security
- ☑ System and Services Acquisitions
- ☑ Supply Chain Risk Management

FBI CJIS Audit of 6.0 Start Date: 10/1/2025

CJIS Security Policy Link

https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center



CJIS 6.1 Update as of June 25, 2026

SUMMARY OF CHANGES

Version 6.1

APB Approved Changes

1. **Addressing Omissions, Corrections, and Additions to the Modernized *CJIS Security Policy* (*CJISSECPOL*) Part 1, Spring 2025, APB#16, SA#1:** update sections with approved changes.
2. **Addressing Omissions, Corrections, and Additions to the Modernized *CJIS Security Policy* (*CJISSECPOL*) Part 2, Spring 2025, APB#16, SA#2:** update sections with approved changes.
3. **Addressing Omissions, Corrections, and Additions to the Modernized *CJIS Security Policy* (*CJISSECPOL*) Part 3, Spring 2025, APB#16, SA#3:** update sections with approved changes.

Administrative Changes

1. **Administrative Changes approved by the Security and Access Subcommittee on November 14, 2025**.

Note: Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

KEY TO APB APPROVED CHANGES (e.g., "**Modernizing Personnel Security (PS) in the *CJISSECPOL*, Spring 2024, APB#11, SA#7:** modernize the CJIS Security Policy requirements for:")

Topic Paper Title
Spring 2024 – Advisory Policy Board cycle and year
APB# – Advisory Policy Board Topic number
SA# – Security and Access Subcommittee Topic number
Summary of change

CA-7 Continuous Monitoring

Requirement (*Priority I)* Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy

System Level Metrics to Be Monitored

- AC-2: Account Management
- AC-17: Remote Access | Monitoring and Control
- AT-4(a): Training records
- CM-3(f): Configuration Change Control
- CM-6(d) Configuration Settings
- CM-11(c): User-Installed Software
- IR-5: Incident Monitoring
- MA-2(b): Controlled Maintenance
- MA-3(a): Maintenance Tool
- MA-4(a): Nonlocal Maintenance
- PE-3(d): Physical Access Control
- PE-6: Monitoring Physical Access
- PE-14(b): Environmental Controls
- PE-16: Delivery and Removal
- PS-7(e): External System Services
- SC-7(a): Boundary Protection
- SC-7(24)(b): Boundary Protection | PII
- SC-18(b): Mobile Code
- SI-4: System Monitoring

CA-7 Continuous Monitoring Cont'd

CA-7 (1): Continuous Monitoring | Independent Assessment
Priority Schedule 1 - Agencies and organizations that manage CJI must employ **independent continuous monitoring** across a range of system to provide more thorough, ongoing awareness.
The level of required independence is based on organizational continuous monitoring strategies.

CA-7 (4): Continuous Monitoring | Risk Monitoring
Priority Schedule 1 - Organizations must ensure that risk monitoring is a documented and imbedded part of the continuous monitoring strategy, which includes;

- Effectiveness monitoring
- Compliance monitoring
- Change monitoring

5.4 Audit & Accountability

- Documented and enforce security policies are required to ensure adherence to accountability controls and ability to detect potentially unauthorized activities
- Includes auditable records for significant events:
  - Authentication, file use, user/group management, log-on attempts, permission changes, and actions on privileged accounts
  - Attempts to access, modify, or destroy audit log files
- Records should include the event type, date, source, outcome, and identity of involved individuals and must be kept for at least (1) year



5.5 Access Control (AC)

Access control policies must define the scope, roles, and responsibilities of personnel, and assign an individual to oversee security policies and procedures

Must be reviewed and updated annually to identify potential security incidents involving unauthorized access to systems and information

Should define and document the types of accounts allowed to access CJI systems and specify those prohibited



5.5 Access Control (AC) Cont’d



- Users must be required to log out when work period is completed
- Sessions must be automatically terminated when a user logs out
- If there is evidence of a significant security or privacy risk, accounts must be disabled within **30 minutes** of discovering threats
- Limit (**5**) consecutive login attempts should be enforced within a 15-minute period to combat credential stuffing and brute force attempts
- If the maximum unsuccessful attempts is exceeded, account should be automatically locked until released by an administrator
- Policies must prohibit use of bring your own device (BYOD), including mobile devices and publicly accessible systems, for accessing, processing, storing, or transmitting CJI data

Account Management

<u>Policies must cover:</u>

- Account creation, enabling, modification, disabling, and removal, and include provisions for monitoring account usage.
- Accounts must be terminated, transferred, or modified within **(1) day** when they are no longer needed or when system usage or need-to-know changes
- Accounts with temporary and emergency access should be automatically removed or disabled within **72 hours**
    - Accounts should be disabled within a week when:
        - The account has expired
        - Are no longer associated with a user or individual
        - Violate organizational policy
        - Have been inactive for 90 calendar days



5.6 Identification & Authentication



Multi-Factor Authentication (MFA) must be implemented for accessing privileged accounts and replay-resistant authentication mechanisms for both privileged and non-privileged accounts



IA policies and procedures must be able to uniquely identify and authenticate agency-managed devices before they can establish network connections



Only approved devices, identified and authenticated prior to connecting to agency assets, should access systems that handle CJI



Reuse of individual system identifiers (e.g., usernames or system accounts assigned to individuals) should be limited to (1) year



Agencies must manage these identifiers by uniquely identifying each individual as either agency or non-agency personnel

5.6 Authenticator Management

- New policies and guidance for session management are designed to securely maintain sessions between a subscriber's software (such as a browser or application) and a relying party (RP) or credential service provider (CSP) without requiring re-authentication for each interaction
- **Key new requirements include:**
  - Session binding
  - Security measures
  - Session integrity
  - Token use



5.10 Denial of Service Protection

- To limit or prevent DoS impacts, polices for controls must include:
  - Monitoring and managing communication at both external and key internal interfaces
  - Using subnetworks for publicly accessible components, separated from internal networks
  - Connecting to external networks only through managed interfaces with boundary protection devices
- The number of external networks connected to CJI related systems should also be limited



5.14 Systems and Services Acquisition

- Agencies will be required to replace system components when support is no longer available from the developer, vendor, or manufacturer
  - Includes when a vendor no longer provides software patches or product updates
    - ➢ Without updated support for these components, adversaries can exploit weaknesses in these installed components
- Alternative support for systems that no longer offer product updates or software patches can be provided by prohibiting connecting vulnerable systems to any public or uncontrolled networks, or by isolating the system or network

5.15 System and Information Integrity

- Agencies must develop policies for testing patches before installation, rollback capabilities, enabling automatic updates, and centralized patch management
- Updates for security-relevant software and firmware must be made within a specified number of days after a patch is released based on the severity of the flaw:
  - 15 days for critical flaws
  - 30 days for high flaws
  - 60 days for medium flaws
  - 90 days for low flaws

Advice: It is always better to manually test and then roll out an update in a controlled fashion to avoid disaster, (i.e; CrowdStrike).

Malicious Code Protection

- Agencies must implement systems that provide signature-based detections that identify malicious codes
- Includes performing periodic scans of the system daily as well as real-time scans of packets from external networks of all entry and endpoint devices for all files that are downloaded, opened or executed, as followed by policies
- Must provide alerts to system or network administrators to take mitigating action when necessary
- Systems must be able to identify false positives during scans to address as well

Spam and Spyware Protection

- Agencies must employ spam protection mechanisms at critical entry points such as
  - Firewalls
  - Email servers
  - Remote-access servers
- Spyware protection must be in place for workstations, servers, and mobile devices
- Mechanisms should detect and take action on unsolicited messages and spyware/adware transported by email, internet accesses, or removable media



5.16 Non-Local Maintenance



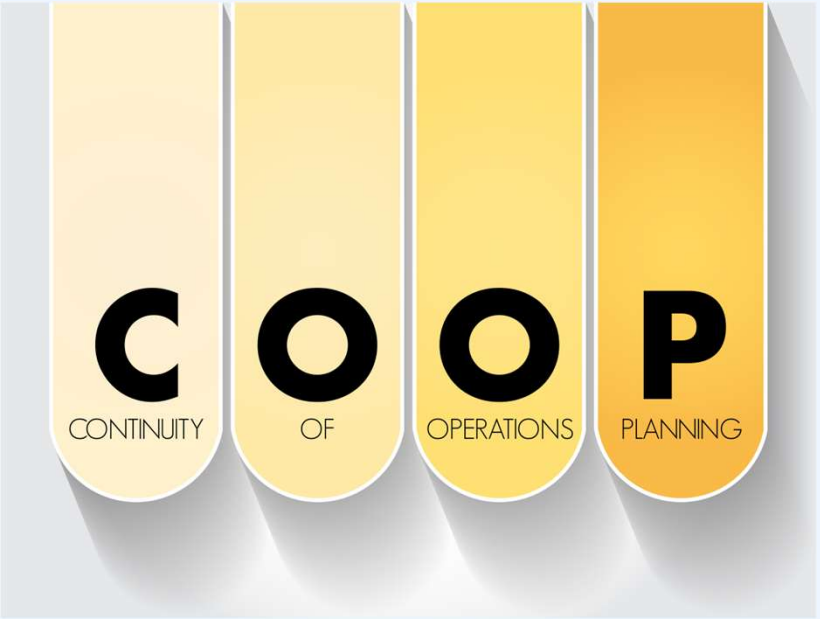
- Develop policies to control all maintenance including
  - Non-local maintenance (remote or network-based):
    - Allow remote tools only as per organizational policy and security plans
    - Use strong authentication for remote sessions
    - Keep records of non-local maintenance activities
    - End sessions and network connections once remote maintenance is complete

5.17 Planning

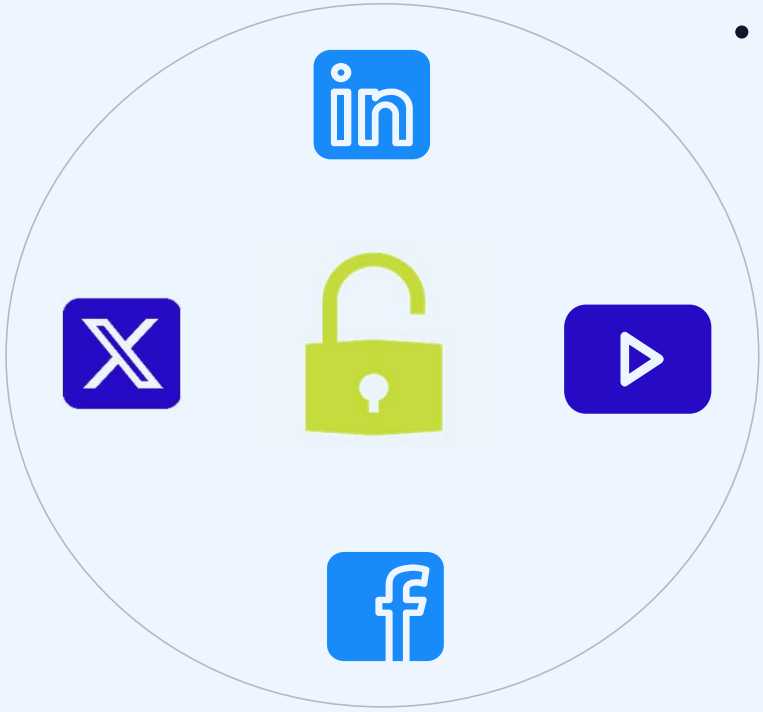
- Organizations must develop comprehensive security and privacy plans for both emergency and non-emergency situations, including **incident response plans**
  - Key elements
    - Definition of system components and operational context
    - Identification of system roles, information types, and security categorization
    - Description of specific threats and privacy risks, especially for systems handling PII
    - Overview of security and privacy requirements, control baselines, and overlays
    - Description of controls in place or planned, with rationale for tailoring decisions
    - Inclusion of risk determinations and coordination activities with relevant personnel
    - Annual review and updates based on system changes or issues

5.18 Contingency Planning

- Agencies must develop **a contingency plan to ensure the continuation of essential operations** in case of system disruptions to:
  - Identify critical functions and contingency requirements
  - Set recovery objectives and priorities
  - Assign roles and responsibilities for contingency actions
  - Plan for maintaining operations during system failures and fully restoring the system
  - Address sharing of contingency information



Rules of Behavior



- Agencies must establish guidelines for using social media and external sites, including restrictions on:
  - Social media and external application usage
  - Posting organizational information publicly
  - Using organizational identifiers, like email addresses and passwords, for external accounts

Security And Privacy Architectures

- Agencies must develop comprehensive security and privacy architectures to
  - Outline strategies for maintaining confidentiality, integrity, and availability of information
  - Detail methods for handling personally identifiable information to minimize privacy risks
- Architectures should be reviewed and updated annually or whenever system or environmental changes occur
- Planned changes must be integrated into security



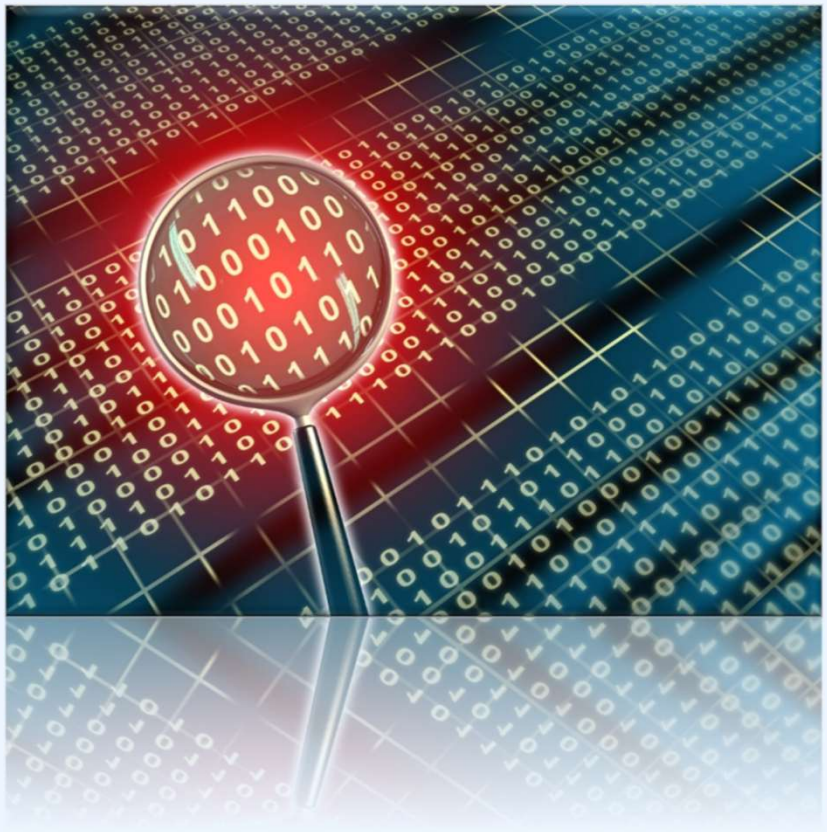
5.19 Risk Assessment



- Develop policies to implement risk assessments for any systems that contain, store, process or transmit CJI
- Systems should be categorized
- Vulnerability scanning and risk assessments must be conducted to identify threats and vulnerabilities in the system
- Monitoring tools should facilitate the ability to process and share information related to software flaws, improper configurations (i.e. firewalls), testing procedures and vulnerability impact, as well as analyzing scan reports from vulnerability monitoring
- Formulate risk response based on findings

Types of Vulnerability Assessments

- Network-Based Scans
- Host-Based Scans
- Wireless Network Scans
- Web Application Scans
- Cloud-Based Scans
- Database Scans



Identification of Threats and Risks

- Identifying threats to the system and vulnerabilities in the system;
- Determine risk or harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system and impact of adverse effects on individuals arising from the processing of PII and CJI
- Integrate risk assessment findings and risk management decisions from both organizational and mission/business perspectives with system-level risk assessments
- Findings should be documented in a risk assessment report, reviewed and updated quarterly, or whenever significant changes occur that might affect the system's security or privacy state



Requirements for Vulnerability Monitoring & Scanning

- Monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported;
- Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process
- Measure vulnerability impact
- Analyze vulnerability scan reports and results from vulnerability monitoring
- Legitimate vulnerabilities must be remediated within the number of days listed;
  - 15 days for critical
  - 30 days for high
  - 60 days for medium
  - 90 days for low

Steps to Compliance

Multifactor Authentication (MFA)

1. **What you carry**
   a. Keys
   b. ID card
   c. Phone

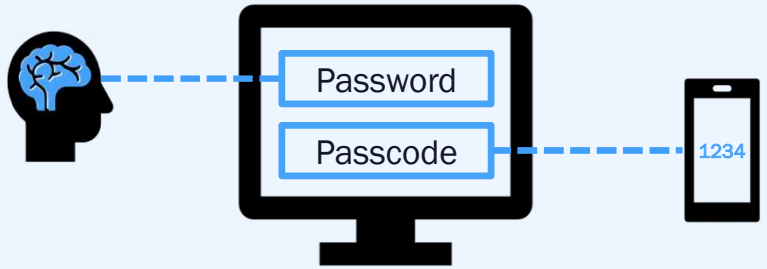
2. **Who you are**
   a. Retinal scan
   b. Fingerprint

3. **What you know**
   a. Passwords

Using more levels increases security

Two-factor authentication example:

1. Enter Password
2. Enter Passcode sent via text or email to phone



Incident Response Planning (IRP)

Be Prepared for the Inevitable

Have a PLAN, Communicate your PLAN and TEST YOUR PLAN!



- Build an incident response playbook broad enough to address major cybersecurity events that need clear steps and procedures.
- Make sure that you involve your vendors and other key personnel in creating the plan.
- **Print your plan.**
- Communicate your plan.
- Test your plan against various cyber incident scenarios.

Vulnerability Risk Assessments

A vulnerability assessment is the process of identifying, analyzing, and evaluating the risks associated with a specific action or event. The aim is to prevent application security defects and reduce the likelihood of potential threats within a company's network and information systems.

4 Benefits of a Risk Assessment

1. Identifies security issues with various internal and external factors
2. Determines new security requirements
3. Creates awareness about risks and measures needed to fix them
4. Better planning of IT structure and resources to create new security plans and policies

Monitor Continuously

Every new account or device creates a risk of misconfiguration, known vulnerabilities, zero day vulnerabilities, and sensitive data exposure

- Examining and testing the attack surface once has limited value, because attack surfaces grow and change every time a new device, user account, workload, or service is added
- It is important to continuously monitor all possible attack vectors against all attack surfaces, and always refer to the most current version of the organization's attack surface



Best Practices and Recommendations

8 Important Evergreen Cybersecurity Lessons

1. It's not if you will be attacked, but when
2. Supply chains are not immune against cyber attacks
3. Cloud security and DNS misconfigurations can invite data breaches
4. Cybersecurity awareness is very crucial – always be aware of your surroundings
5. Patch, patch, and patch; make sure systems are up to date
6. Adopting zero trust methodologies is recommended
7. Cyber Hygiene training is critical for protecting your network. Your personnel are your first line of defense
8. 24x7x365 cybersecurity monitoring is a requirement



10 Key Cyber Policies

1. Acceptable use
2. Authentication
3. Password Management
4. Email Use
5. Social Media
6. Remote Access
7. End Point Protection
8. Data Storage
9. Continuous Monitoring
10. Identity Access Management



Utilize Resources

Sign-Up for the PSTA
https://namrinfo.motorolasolutions.com/join-the-psta

CISA Known Exploited Vulnerabilities:
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

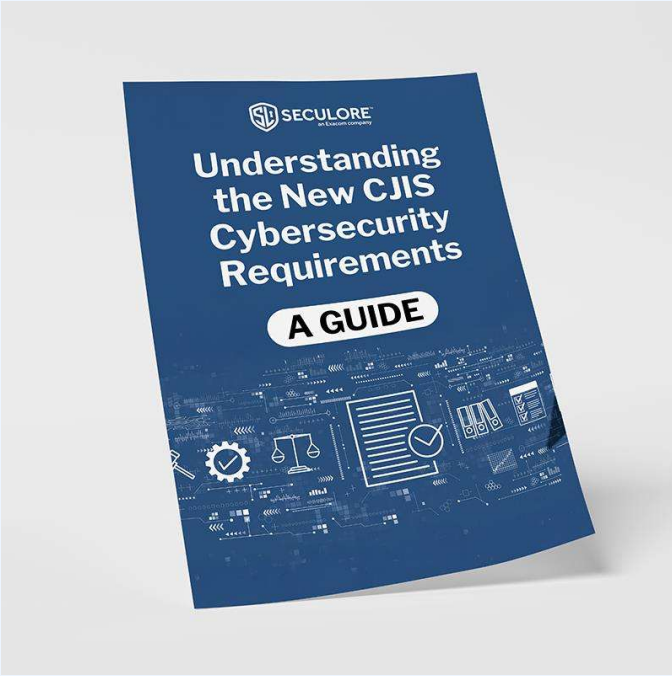
Nation-State Cyber Actors
https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors



Free Resource

Understanding the New CJIS Cybersecurity Requirements: A Guide

Additional information on the latest policy updates to the Criminal Justice Information Services (CJIS) cybersecurity requirements and actionable recommendations to meet compliance.



Thank You!

Have any questions?
We're Here to Help

Frank Arico
frank.arico@motorolasolutions.com
847.875.2400 mobile #

Angie Wineland
angie.wineland@motorolasolutions.com
720.935.6198 mobile #

COLORADO
9-1-1 PROGRAM

SECULORE®
a Motorola Solutions Company