Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Division

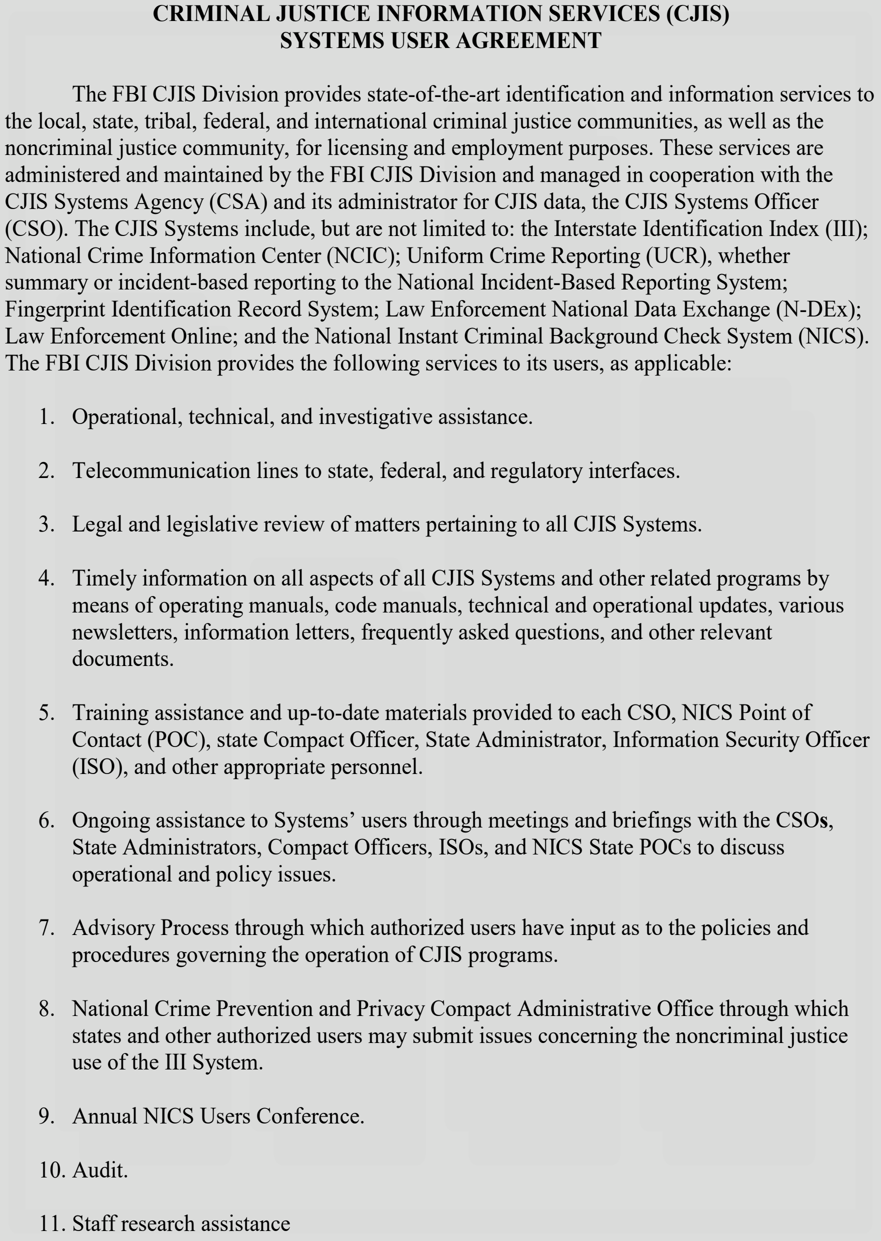
Information Security Officer (ISO) Conference Advisory Process Overview

Shared Management Concept

- Federal, state, local, and tribal users and providers share the responsibility for the operation and management of systems administered by the CJIS Division for the benefit of the criminal justice community.

CJIS Advisory Process

- Process to obtain the user community's guidance on the operation of CJIS programs.



CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Online; and the National Instant Criminal Background Check System (NICS). The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.
2. Telecommunication lines to state, federal, and regulatory interfaces.
3. Legal and legislative review of matters pertaining to all CJIS Systems.
4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.
5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.
6. Ongoing assistance to Systems' users through meetings and briefings with the CSOs, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.
7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.
8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.
9. Annual NICS Users Conference.
10. Audit.
11. Staff research assistance

FBI FEDERAL BUREAU OF INVESTIGATION

National Crime Information Center (NCIC) APB

- Established in 1969 to recommend general policy with respect to the philosophy, concept and operational principles of a nationwide law enforcement system, particularly its relationships with local and state systems

- Original membership began with 14 regional representatives

- Evolved to include the FBI Director’s appointees representing the judicial, prosecutorial, and correctional sectors, as well as the International Association of Chiefs of Police (IACP), the National Sheriffs’ Association (NSA), the American Probation and Parole Association (APPA) and the National District Attorneys Association (NDAA).

Uniform Crime Reporting (UCR) APB

- Established in 1989, under the Federal Advisory Committee Act.
- UCR Membership included the following:
  - Nine IACP nominations.
  - Five NSA nominations
  - Two National Academy Associate nominations
  - Four appointments made by the FBI Director

CJIS APB

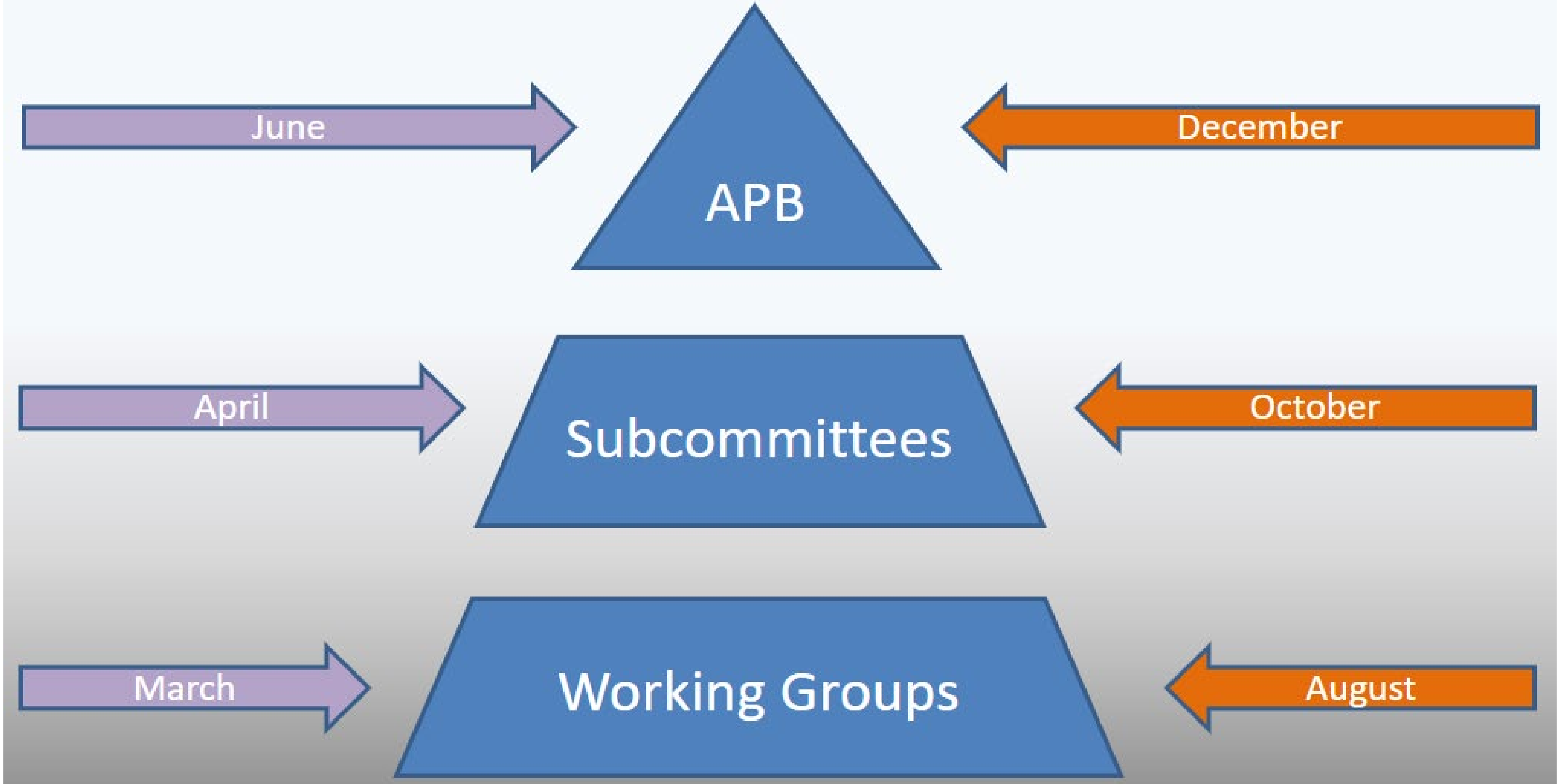
- Established in the fall of 1994 by FBI Director Louis J. Freeh to provide recommendations on all programs administered by the FBI's CJIS Division.

- Meetings comply with the FACA

- Concept outlined in the Code of Federal Regulations.

- Group provides recommendations to the FBI Director on CJIS-managed systems and services to include the NCIC, the UCR, Next Generation Identification, National Data Exchange (N-DEx), Law Enforcement Enterprise Portal, and the National Instant Criminal Background Check System (NICS)

Three Main Components of the Advisory Process



June

December

APB

April

October

Subcommittees

March

August

Working Groups

CJIS APB REGIONS

Designated Federal Officer (DFO) Nicky J. Megna
Work Phone: 304-625-2767; Cell: 304-672-0516
njmegna@fbi.gov

Alternate DFO
Stacey Davis
304-625-2618
scdavis2@fbi.gov

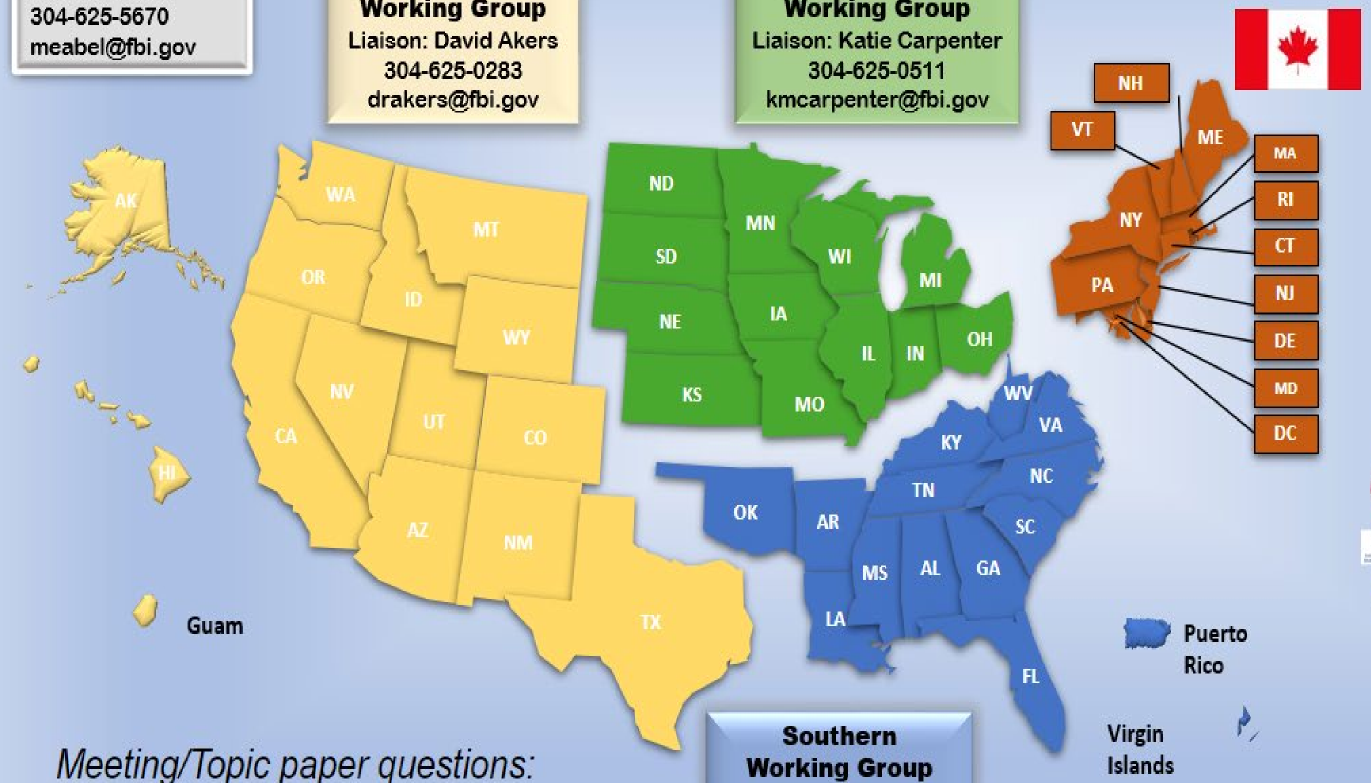
Team Leader
Melissa Abel
304-625-5670
meabel@fbi.gov

Team MPA/Travel
Sandra Porter
304-625-4279
sjporter@fbi.gov

Western Working Group
Liaison: David Akers
304-625-0283
drakers@fbi.gov

North Central Working Group
Liaison: Katie Carpenter
304-625-0511
kmcarpenter@fbi.gov

Northeastern Working Group
Liaison: Ryan Lemley
304-625-8952
rplemley@fbi.gov



Federal Working Group
Liaison: June Fahey
304-625-5234
jmfahey@fbi.gov

Southern Working Group
Liaison: Jill Plybon
304-625-5424
jlplybon@fbi.gov

Meeting/Topic paper questions:
Agmu@leo.gov

Advisory Process Subcommittees

- Identification Services
- Data Sharing Services
- NCIC
- Compliance Evaluation
- Security and Access
- UCR
- NICS
- Public Safety and Strategy
- Executive
- Bylaws

CJIS Advisory Policy Board

Thirty-five members appointed by the FBI Director comprised of:

- 20 members nominated by the four regional working groups.
- One member nominated by the Federal Working Group.
- Five members selected by the FBI Director representing the prosecutorial, judicial and correctional sectors, as well as the tribal and national security communities.
- One member from each of the following criminal justice professional associations:
  - International Association of Chiefs of Police
  - National Sheriffs' Association
  - Major Cities Chiefs
  - American Society of Crime Laboratory Directors
  - Representative from the courts or court administrators selected by the Conference of Chief Justices
  - National District Attorneys' Association
  - American Probation and Parole
  - Major County Sheriffs of America
- One member selected by the Chair of the National Crime Prevention and Privacy Compact Council.

Current APB Leadership

APB Chair

Kathy Witt

Sheriff

Sheriff Office of

Fayette County

Lexington, Kentucky

APB Vice Chair

Charles "Monty" Coats, Jr.

Major

South Carolina

Law Enforcement Division
Columbia, South Carolina

APB 2nd Vice Chair

Brian Wallace

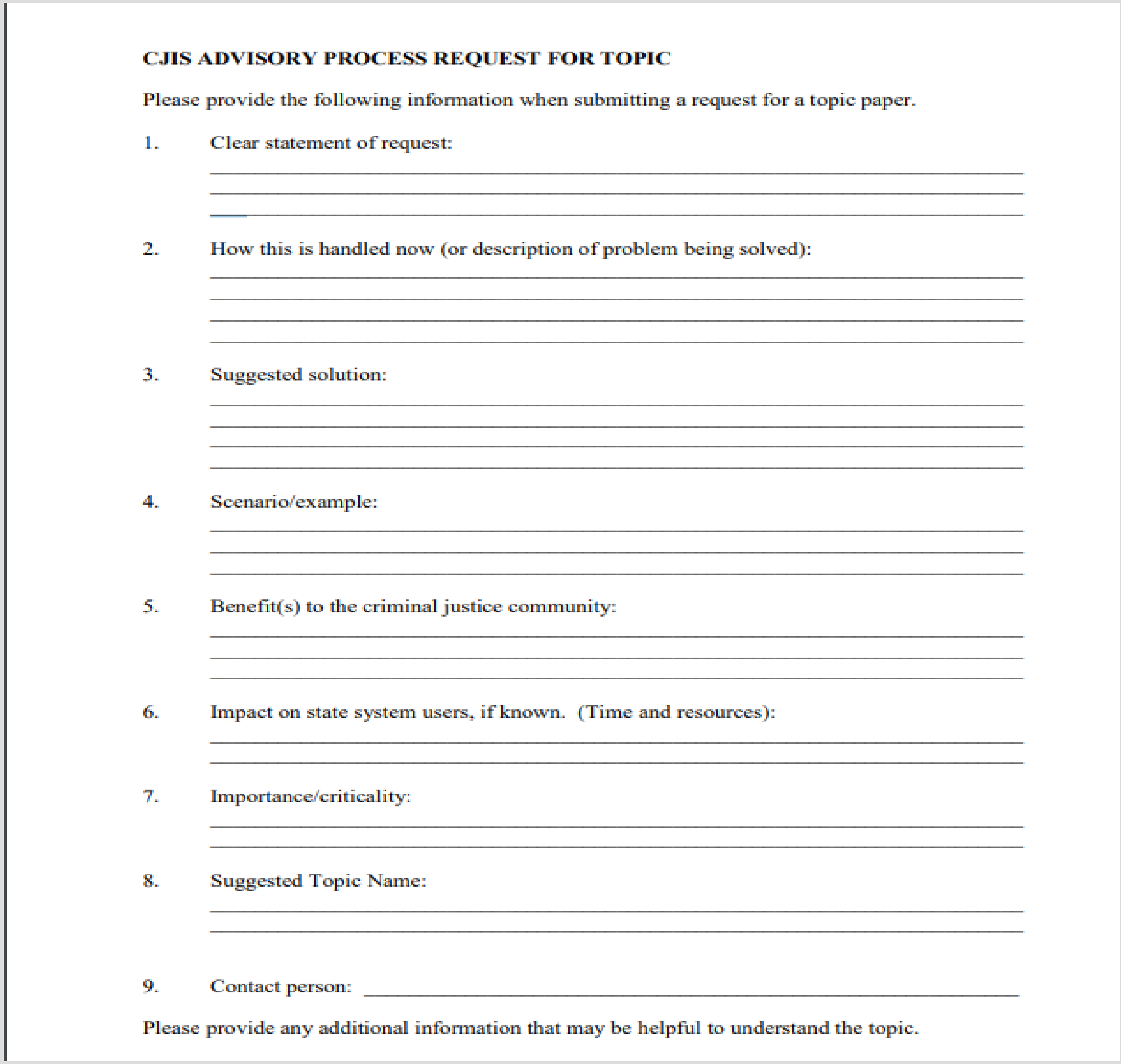
Chief Civil Deputy

Marion County

Sheriff's Office

Salem, Oregon

Sample Topic Paper Submission



CJIS ADVISORY PROCESS REQUEST FOR TOPIC

Please provide the following information when submitting a request for a topic paper.

1. Clear statement of request:

____
____
____

2. How this is handled now (or description of problem being solved):

____
____
____
____

3. Suggested solution:

____
____
____
____

4. Scenario/example:

____
____
____

5. Benefit(s) to the criminal justice community:

____
____
____

6. Impact on state system users, if known. (Time and resources):

____
____

7. Importance/criticality:

____
____

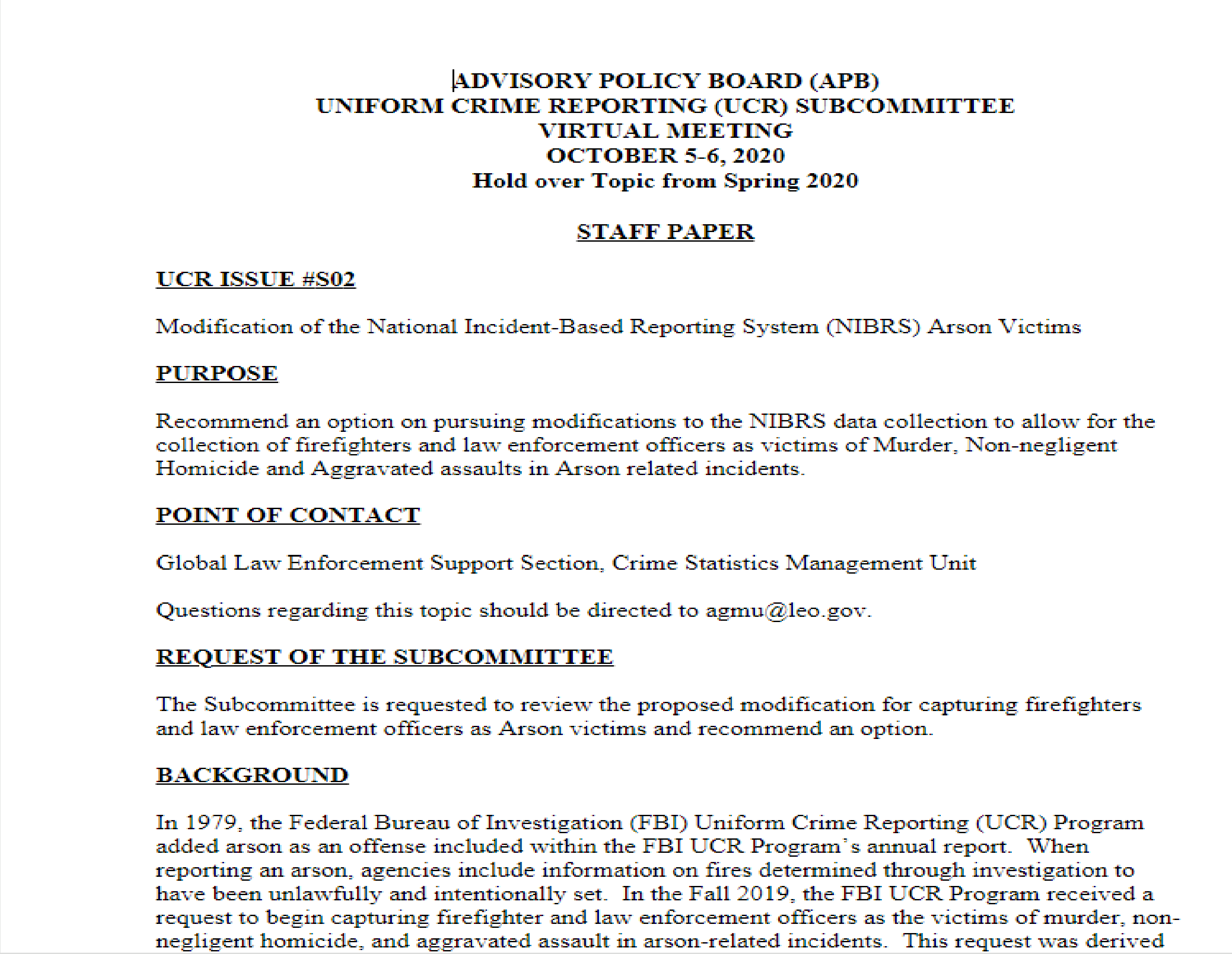
8. Suggested Topic Name:

____
____

9. Contact person: ____

Please provide any additional information that may be helpful to understand the topic.

Sample Topic Paper



ADVISORY POLICY BOARD (APB)
UNIFORM CRIME REPORTING (UCR) SUBCOMMITTEE
VIRTUAL MEETING
OCTOBER 5-6, 2020
Hold over Topic from Spring 2020

STAFF PAPER

UCR ISSUE #S02

Modification of the National Incident-Based Reporting System (NIBRS) Arson Victims

PURPOSE

Recommend an option on pursuing modifications to the NIBRS data collection to allow for the collection of firefighters and law enforcement officers as victims of Murder, Non-negligent Homicide and Aggravated assaults in Arson related incidents.

POINT OF CONTACT

Global Law Enforcement Support Section, Crime Statistics Management Unit

Questions regarding this topic should be directed to agmu@leo.gov.

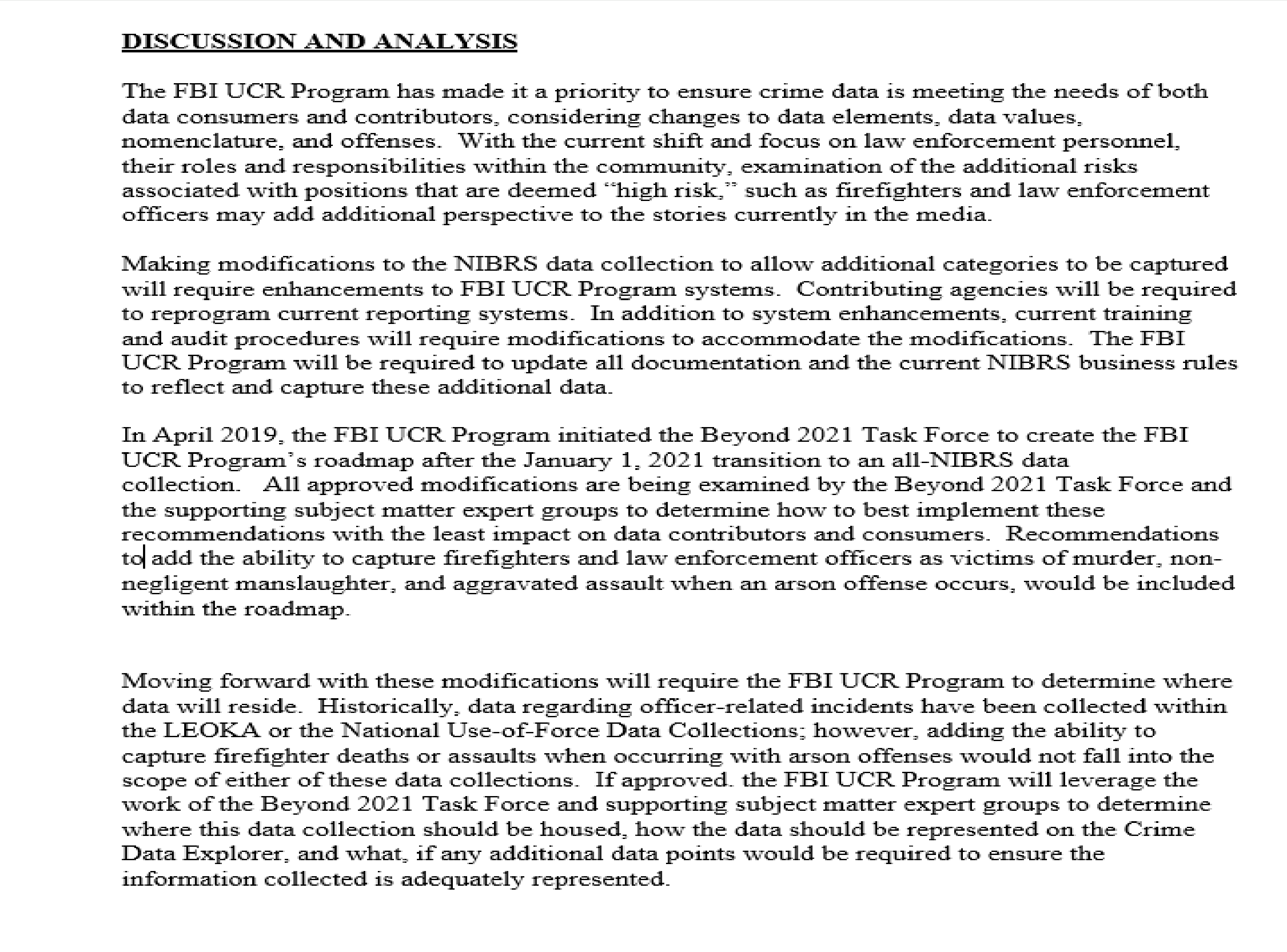
REQUEST OF THE SUBCOMMITTEE

The Subcommittee is requested to review the proposed modification for capturing firefighters and law enforcement officers as Arson victims and recommend an option.

BACKGROUND

In 1979, the Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Program added arson as an offense included within the FBI UCR Program's annual report. When reporting an arson, agencies include information on fires determined through investigation to have been unlawfully and intentionally set. In the Fall 2019, the FBI UCR Program received a request to begin capturing firefighter and law enforcement officers as the victims of murder, non-negligent homicide, and aggravated assault in arson-related incidents. This request was derived

Sample Topic Paper continued…



DISCUSSION AND ANALYSIS

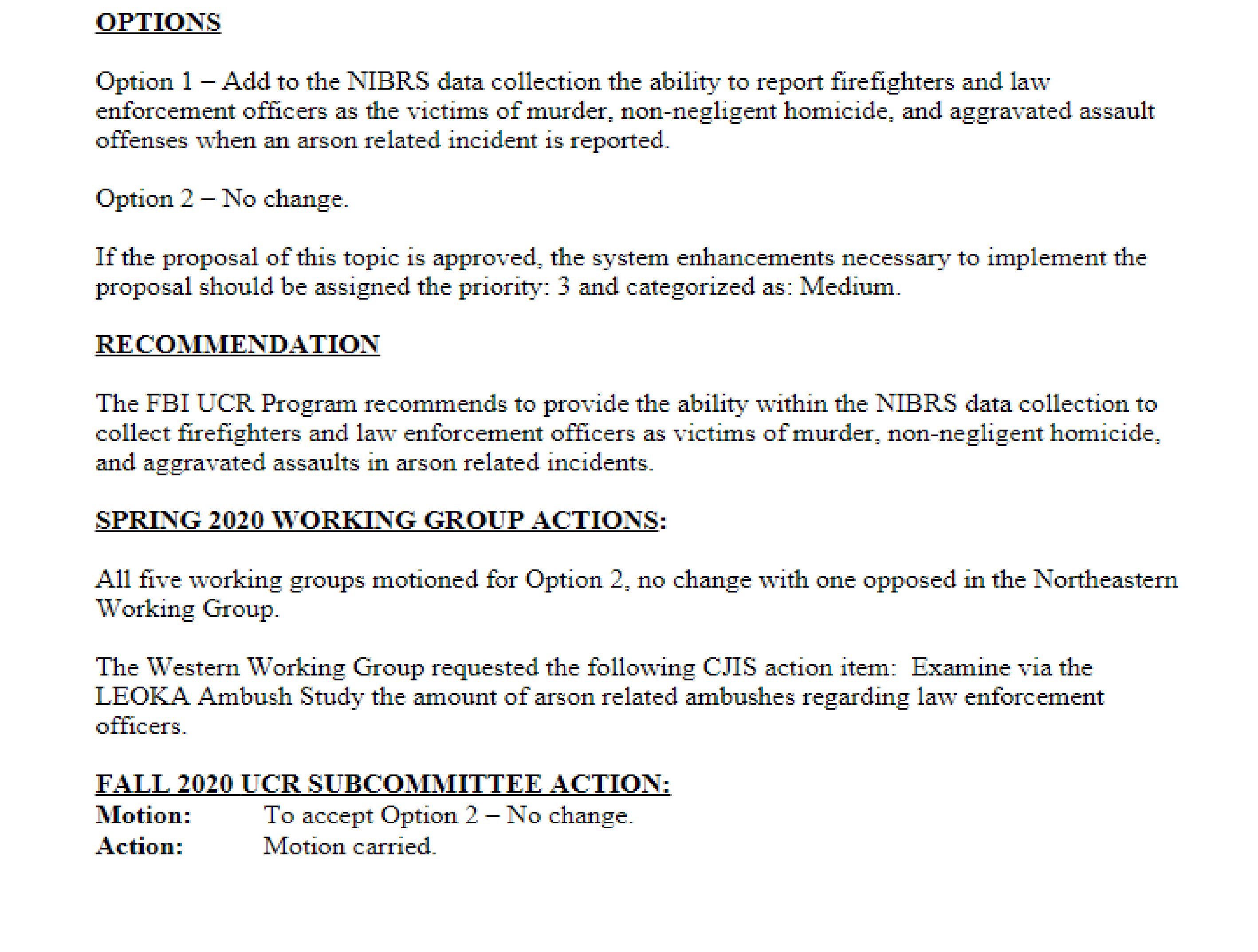
The FBI UCR Program has made it a priority to ensure crime data is meeting the needs of both data consumers and contributors, considering changes to data elements, data values, nomenclature, and offenses. With the current shift and focus on law enforcement personnel, their roles and responsibilities within the community, examination of the additional risks associated with positions that are deemed "high risk," such as firefighters and law enforcement officers may add additional perspective to the stories currently in the media.

Making modifications to the NIBRS data collection to allow additional categories to be captured will require enhancements to FBI UCR Program systems. Contributing agencies will be required to reprogram current reporting systems. In addition to system enhancements, current training and audit procedures will require modifications to accommodate the modifications. The FBI UCR Program will be required to update all documentation and the current NIBRS business rules to reflect and capture these additional data.

In April 2019, the FBI UCR Program initiated the Beyond 2021 Task Force to create the FBI UCR Program's roadmap after the January 1, 2021 transition to an all-NIBRS data collection. All approved modifications are being examined by the Beyond 2021 Task Force and the supporting subject matter expert groups to determine how to best implement these recommendations with the least impact on data contributors and consumers. Recommendations to add the ability to capture firefighters and law enforcement officers as victims of murder, non-negligent manslaughter, and aggravated assault when an arson offense occurs, would be included within the roadmap.

Moving forward with these modifications will require the FBI UCR Program to determine where data will reside. Historically, data regarding officer-related incidents have been collected within the LEOKA or the National Use-of-Force Data Collections; however, adding the ability to capture firefighter deaths or assaults when occurring with arson offenses would not fall into the scope of either of these data collections. If approved. the FBI UCR Program will leverage the work of the Beyond 2021 Task Force and supporting subject matter expert groups to determine where this data collection should be housed, how the data should be represented on the Crime Data Explorer, and what, if any additional data points would be required to ensure the information collected is adequately represented.

Sample Topic Paper continued…



OPTIONS

Option 1 – Add to the NIBRS data collection the ability to report firefighters and law enforcement officers as the victims of murder, non-negligent homicide, and aggravated assault offenses when an arson related incident is reported.

Option 2 – No change.

If the proposal of this topic is approved, the system enhancements necessary to implement the proposal should be assigned the priority: 3 and categorized as: Medium.

RECOMMENDATION

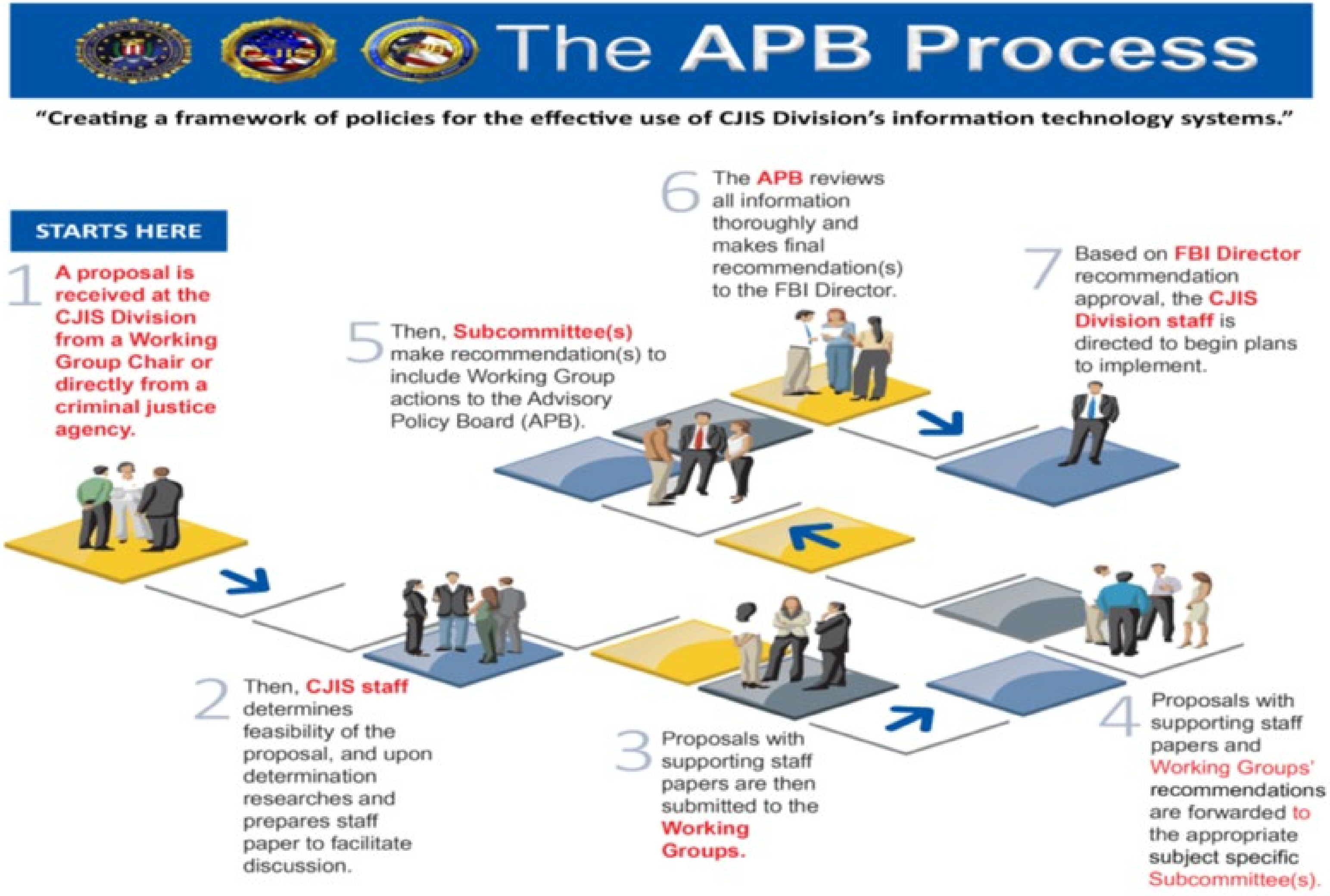
The FBI UCR Program recommends to provide the ability within the NIBRS data collection to collect firefighters and law enforcement officers as victims of murder, non-negligent homicide, and aggravated assaults in arson related incidents.

SPRING 2020 WORKING GROUP ACTIONS:

All five working groups motioned for Option 2, no change with one opposed in the Northeastern Working Group.

The Western Working Group requested the following CJIS action item: Examine via the LEOKA Ambush Study the amount of arson related ambushes regarding law enforcement officers.

FALL 2020 UCR SUBCOMMITTEE ACTION:
Motion: To accept Option 2 – No change.
Action: Motion carried.



The APB Process

"Creating a framework of policies for the effective use of CJIS Division's information technology systems."

STARTS HERE

1 **A proposal is received at the CJIS Division from a Working Group Chair or directly from a criminal justice agency.**

2 Then, **CJIS staff** determines feasibility of the proposal, and upon determination researches and prepares staff paper to facilitate discussion.

3 Proposals with supporting staff papers are then submitted to the **Working Groups.**

4 Proposals with supporting staff papers and Working Groups' recommendations are forwarded to the appropriate subject specific Subcommittee(s).

5 Then, **Subcommittee(s)** make recommendation(s) to include Working Group actions to the Advisory Policy Board (APB).

6 The **APB** reviews all information thoroughly and makes final recommendation(s) to the FBI Director.

7 Based on **FBI Director** recommendation approval, the **CJIS Division staff** is directed to begin plans to implement.

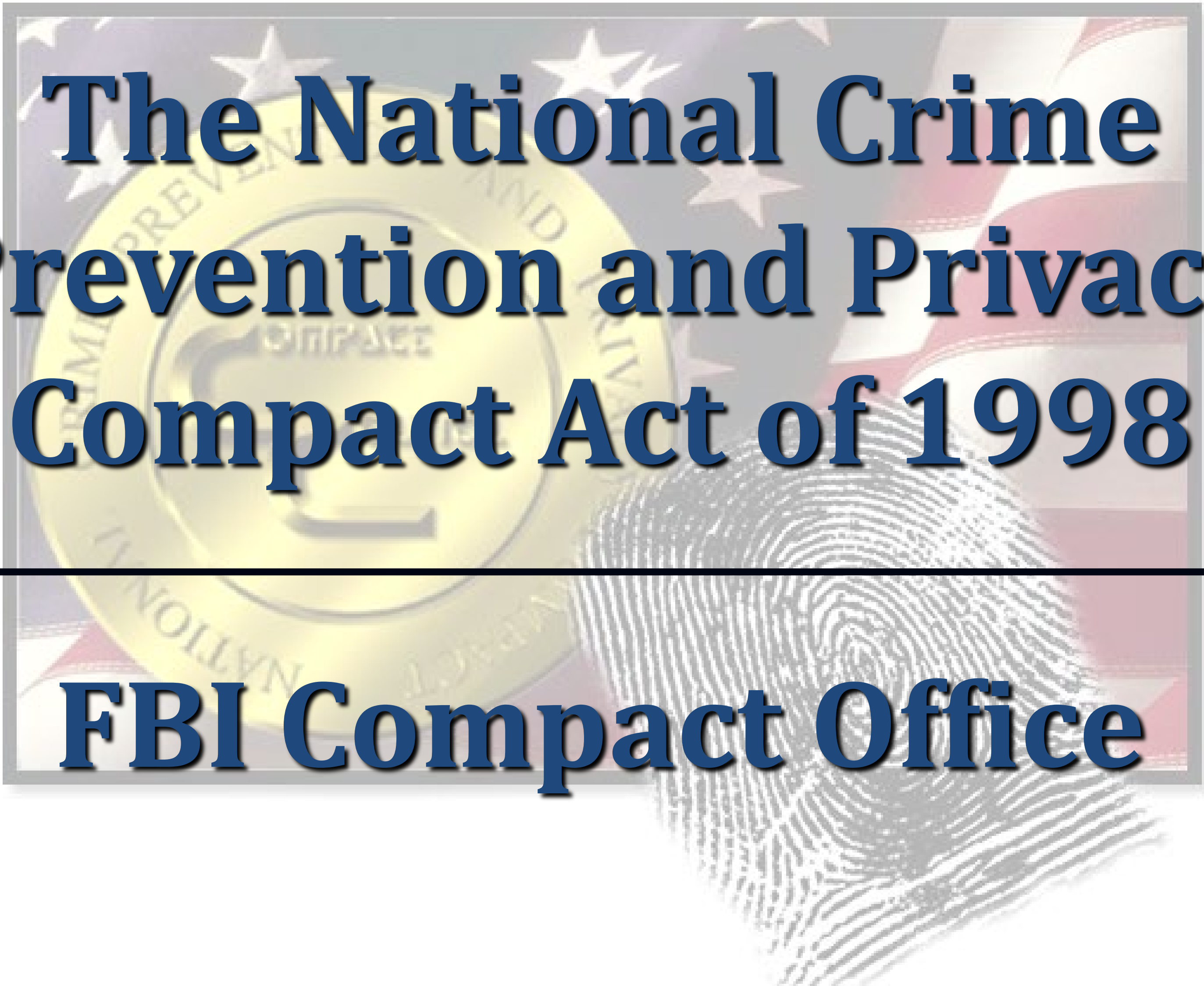
CJIS APB

The CJIS APB's Shared Management Works

- More than 2,400 Recommendations to Date with a 98% Implementation Rate and Counting.
- Strong Partnerships for the FBI and the CJIS Division.
- Considered by Many to be the Gold Standard in FACs.

Questions?

Nicky J. Megna
Designated Federal Officer
FBI CJIS Division
Phone: 304-625-2767
E-mail: <njmegna@fbi.gov>



The National Crime Prevention and Privacy Compact Act of 1998

FBI Compact Office

To enhance public safety through noncriminal justice background checks based on positive identification, while protecting individual privacy rights.

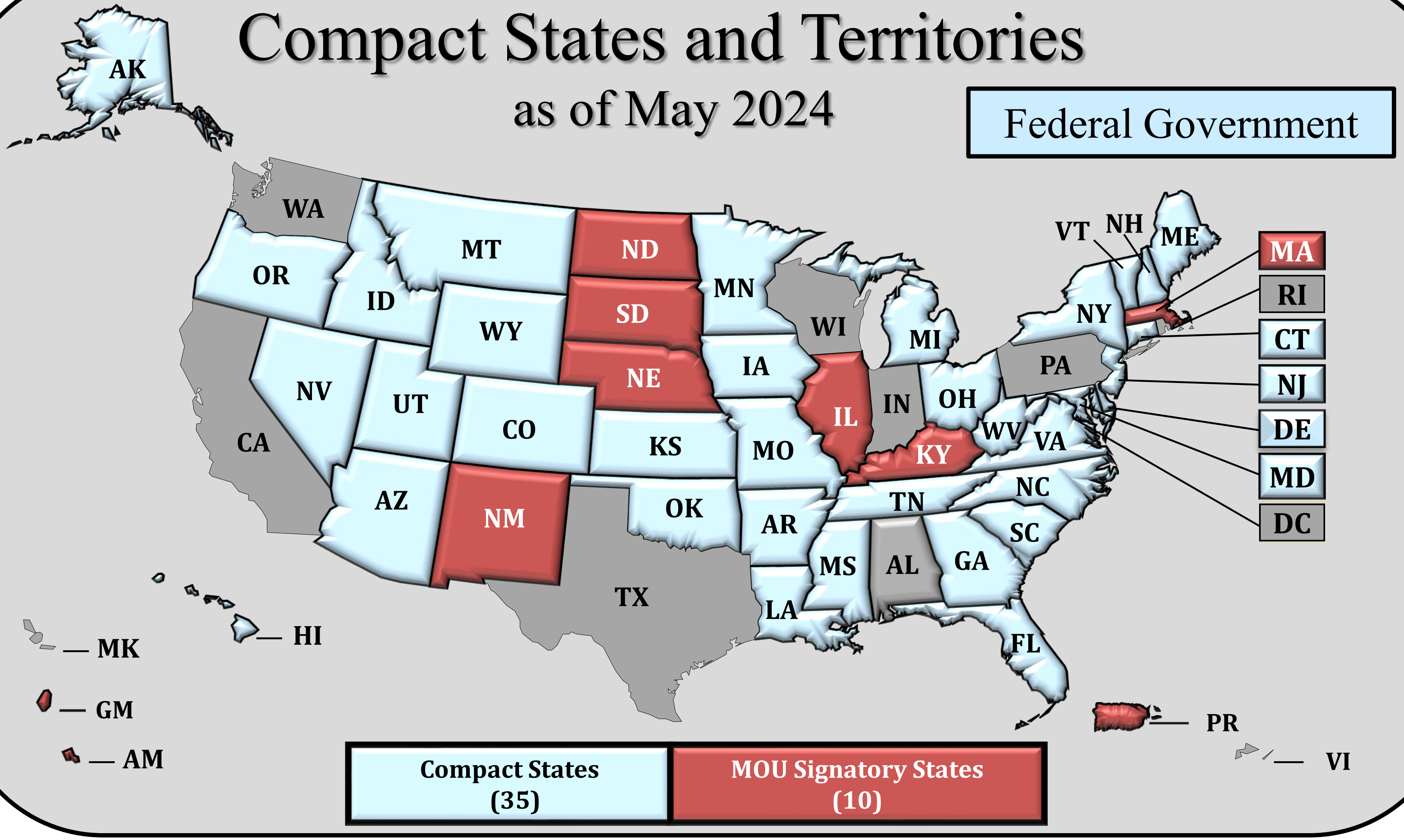
Compact Act

- Implemented on October 9, 1998
  - 34 U.S.C. 40311 – 40316
- Provides legal framework for noncriminal justice use of Interstate Identification Index (III)
- Promotes assurance of record availability
- Safeguards strong state role for decisions regarding state data

History of the Compact Act

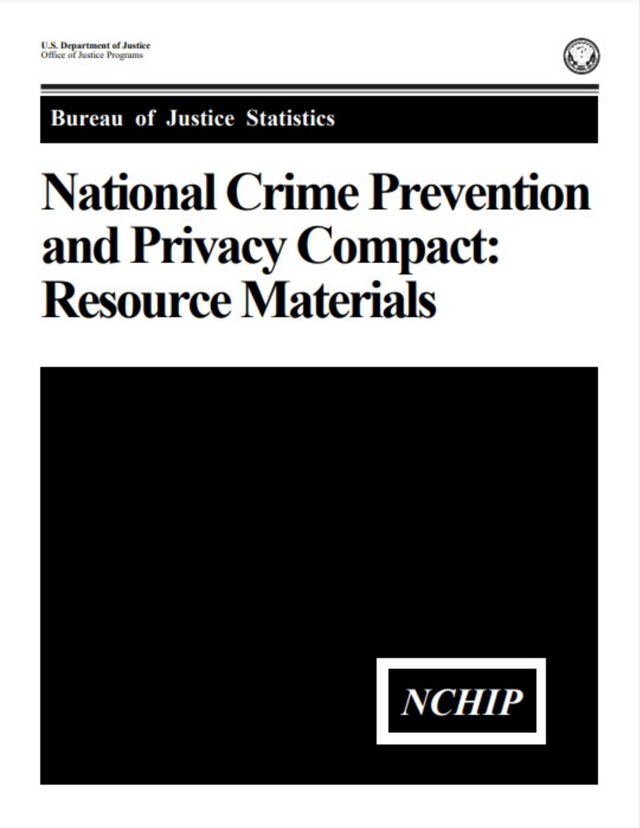
- Continues decentralization of criminal history record information (CHRI)
- Use and dissemination of CHRI for noncriminal justice purposes
  - *purposes authorized by Federal or State law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances*
- Established the Compact Council

Who Participates Today?



Compact Officer Responsibilities

- Responsibilities of each Compact State and the FBI are outlined in Article III of the Compact.
- Each Compact State must appoint a State Compact Officer.
- The FBI Director must appoint an FBI Compact Officer.



U.S. Department of Justice
Office of Justice Programs

Bureau of Justice Statistics

National Crime Prevention and Privacy Compact: Resource Materials

NCHIP

Establishment of the Council

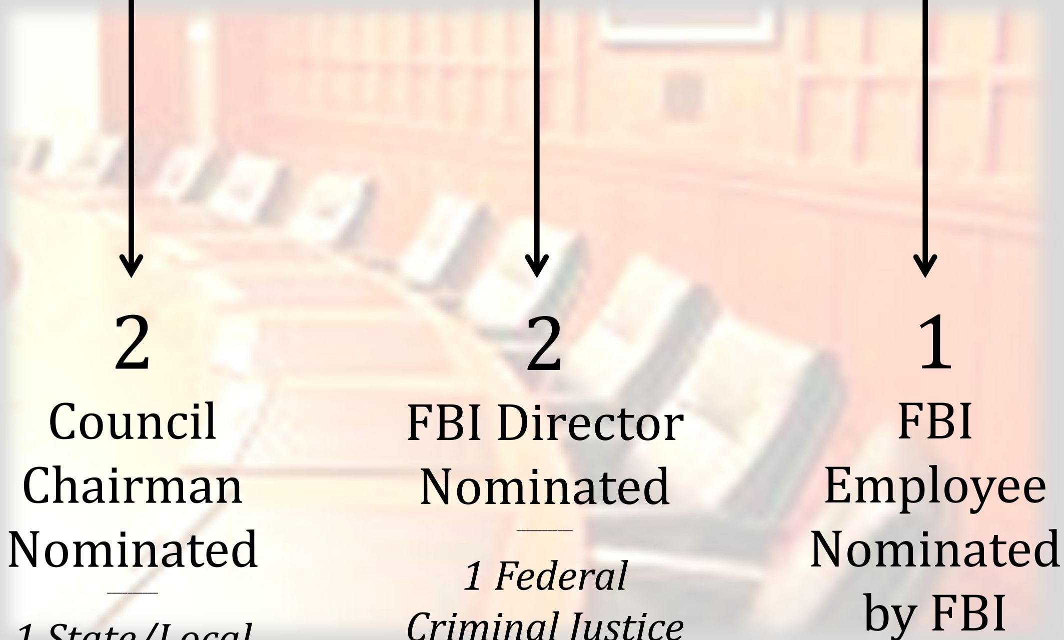
- Article VI of the Compact established the Council.
- Authority to promulgate rules and procedures for the use of the III system for noncriminal justice purposes.
- The Council may only promulgate rules and procedures based on existing statutory authority

Council's Role

- The Council monitors the use of the III system for noncriminal justice purposes to ensure an individual's privacy.
- Not to conflict with the FBI's administration of the III system for criminal justice purposes
- Council will exist as long as the Compact remains in effect

Council's Membership

15 members appointed by the U.S. Attorney General



9
State Compact Officers

2
Council Chairman Nominated

1 State/Local Criminal Justice

1 State/Local Noncriminal Justice

2
FBI Director Nominated

1 Federal Criminal Justice

1 Federal Noncriminal Justice

1
FBI Employee Nominated by FBI Director

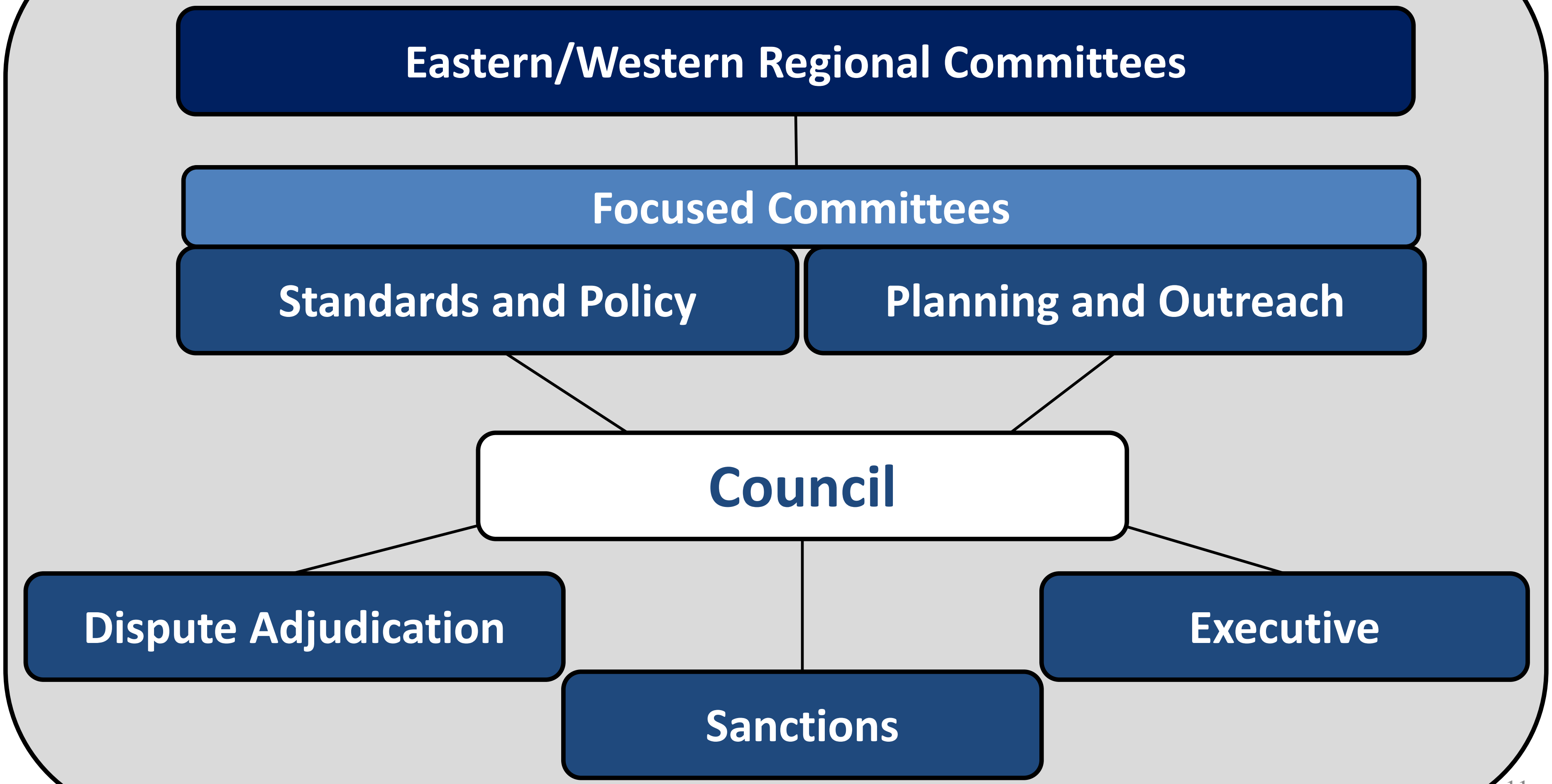
1
APB Member Nominated by APB

Council Leadership

Council Vice Chairman
Charles Murphy
Florida Department of Law Enforcement

Council Chairman
Jason Bright
Montana
Department of Justice

How does the Council Conduct Business?



Eastern/Western Regional Committees

Focused Committees

Standards and Policy

Planning and Outreach

Council

Dispute Adjudication

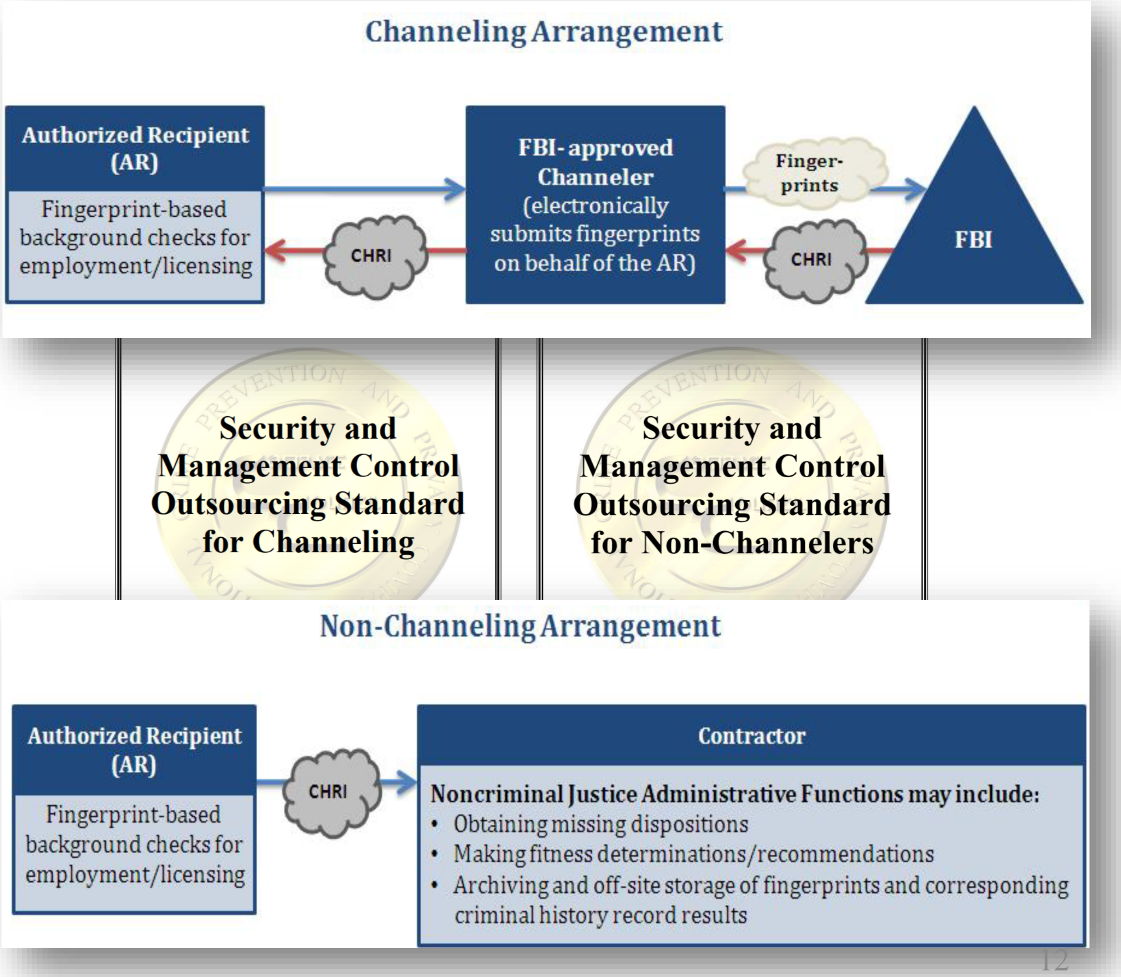
Sanctions

Executive

Outsourcing of Noncriminal Justice Administrative Functions

28 CFR Part 906

- Allows authorized recipients to privatize the submission of noncriminal justice background checks and noncriminal justice administrative functions when approved
- Provides standards to ensure the protection and privacy of the data



Channeling Arrangement

Authorized Recipient (AR)

Fingerprint-based background checks for employment/licensing

CHRI

FBI-approved Channeler (electronically submits fingerprints on behalf of the AR)

Finger-prints

CHRI

FBI

Security and Management Control Outsourcing Standard for Channeling

Security and Management Control Outsourcing Standard for Non-Channelers

Non-Channeling Arrangement

Authorized Recipient (AR)

Fingerprint-based background checks for employment/licensing

CHRI

Contractor

Noncriminal Justice Administrative Functions may include:

- Obtaining missing dispositions
- Making fitness determinations/recommendations
- Archiving and off-site storage of fingerprints and corresponding criminal history record results

Questions?

FBI Compact Officer:

Chasity S. Anderson, csanderson@fbi.gov

Compact Office

Anissa C. Drabish, SMAPA, acdrabish@fbi.gov
Timothy Neal, SMAPA, tneal@fbi.gov

Compact/NFF Team E-mail: compactoffice@fbi.gov

Outsourcing Team E-mail: outsourcing.question@fbi.gov

Compact Council's Website: www.fbi.gov/compactcouncil

CHRIS WEATHERLY

INFORMATION SECURITY OFFICER

FBI/CJIS DIVISION

JEFF CAMPBELL

DEPUTY ISO

FBI/CJIS DIVISION

HOLDEN CROSS

SR. TECHNICAL ANALYST

CJIS SECURITY POLICY

CJIS SECURITY POLICY
Overview

- Fully vetted by all state representation
- Criminal and non-criminal (civil) agencies
- Accompanying *Requirements Companion Document*
- Protect Criminal Justice Information (CJI)
- Identifying the user vs. the device
- Knowing where the user is located
    - Technical controls as well as physical and personnel controls
- Multi-factor authentication

NON-TECHNICAL REQUIREMENTS (SECTIONS 1-4)

CJIS SECURITY POLICY OVERVIEW

Sections 1 – 4

Introduces the CJIS Security Policy, describes the approach used throughout the document, and defines roles and responsibilities

- Community of Criminal Justice Information (CJI)
    - State, county, local, territory, tribe, federal, international criminal justice AND non-criminal justice
    - Private industry
- CJI extends the protection measures of information beyond CHRI to include PII

CJIS SECURITY POLICY OVERVIEW

Section 1 – Introduction

Purpose
Minimum set of security requirements for access to FBI CJIS systems and information and to protect and safeguard CJI

Scope
Applicable to all entities with access to, or who operate in support of, FBI CJIS services and information

Relationship to Local Security Policy and Other Policies
Sole agency security policy or agency may augment with local policy

Terminology
Information and data both refer to CJI

CJIS SECURITY POLICY OVERVIEW

Section 2 – CJIS Security Policy Approach

Vision Statement

Business needs for confidentiality, integrity, and availability of information

Architecture Independent

Data protection centric vice implementation architecture

Risk Versus Realism

Requirements scrutinized for risk versus the reality of resource constraints and real-world application

CJIS SECURITY POLICY OVERVIEW

Section 3 – Roles and Responsibilities

3.2.2 CJIS Systems Officer (CSO)

The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community. (includes sub-bullets a – h)
3. Outsourcing of criminal justice functions (includes sub-bullets a – b).

CJIS SECURITY POLICY OVERVIEW

Section 3 – Roles and Responsibilities

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

CJIS SECURITY POLICY OVERVIEW

Section 3 – Roles and Responsibilities

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

CJIS SECURITY POLICY OVERVIEW

Section 4 – Criminal Justice Information and Personally Identifiable Information

Criminal Justice Information (CJI) – is the term used to refer to all the FBI 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.

The intent of the CJIS Security Policy is to ensure the protection of CJI until such time as the information is either released to the public via authorized dissemination (e.g., within a court system or when presented in crime reports data) or is purged or destroyed in accordance with applicable record retention rules.

Criminal History Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Personally Identifiable Information (PII) — PII is 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.

INFORMATION EXCHANGE AGREEMENTS (5.1)

Section 5.1

Policy Area 1: Information Exchange Agreements

Ensure all parties understand and agree to:

- Required controls
- Responsibilities
- Roles
- Ownership
- Handling

Document the agreement

Section 5.1

Policy Area 1: Information Exchange Agreements

- State and Federal Agency User Agreements
- CJA User Agreements
- Inter-agency and Management Control Agreements
- Agency User Agreements (Civil)
- Security Addendum / Outsourcing Standards

AWARENESS & TRAINING (AT)

AWARENESS AND TRAINING (AT)

- *AT-1: POLICY and PROCEDURES*
- *AT-2: LITERACY TRAINING AND AWARENESS*
  - *Prior to getting access and ANNUALLY thereafter*
  - *Within 30 days of an incident*
  - *Posters, Inscribed Products, Email Advisories, Logon Messages*
  - *Insider Threat*
  - Social Engineering and Social Mining
- AT-3: ROLE BASED TRAINING
  - Unescorted Access
  - General User
  - Privileged User
  - Personnel w/ Information Security Responsibilities
  - *Personally Identifiable Information*
    - *The employment and operation of personally identifiable information processing and transparency controls*

AWARENESS AND TRAINING (AT)

- AT-4: TRAINING RECORDS
  - Document the training
  - *Maintain the records for three years*

INCIDENT RESPONSE (IR)

INCIDENT RESPONSE (IR)

- *IR-1: POLICY AND PROCEDURES*
  - *Annual review*
- *IR-2: INCIDENT RESPONSE TRAINING*
  - *Provide incident response training to system users consistent with assigned roles and responsibilities:*
    - *Prior to assuming an incident response role or responsibility or acquiring system access*
    - *When required by system changes; and*
    - *Annually thereafter; and*
  - *Review and update incident response training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI*

INCIDENT RESPONSE (IR)

- *IR-2(3): BREACH*
  - *Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.*
- *IR-3: INCIDENT RESPONSE TESTING*
  - *Test the effectiveness of the incident response capability*
    - *Tabletop or walk-through exercises*
    - *Simulations; or*
    - *Other agency-appropriate tests.*
- *IR-3(2): COORDINATE WITH RELATED PLANS*
  - *Coordinate incident response testing with organizational elements responsible for related plans.*

INCIDENT RESPONSE (IR)

- *IR-4: INCIDENT HANDLING*
  - *Implement an incident handling capability for incidents that includes:*
    - *Preparation*
    - *Detection and analysis*
    - *Containment*
    - *Eradication, and*
    - *Recovery;*
  - *Coordinate incident handling activities with contingency planning activities;*
  - *Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and*
  - *Ensure the rigor, intensity, scope, and results of incident handling activities are* comparable and predictable across the organization.

INCIDENT RESPONSE (IR)

- *IR-4(1): AUTOMATED INCIDENT HANDLING PROCESSES*
  - Support the incident handling process using automated mechanisms
    - Examples
      - online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis
- *IR-5: INCIDENT MONITORING*
  - *Track and document incidents*
    - *Maintain records*
    - *Sources include:*
      - *Network monitoring*
      - *Incident Reports*
      - *Response Teams*
      - *Users*
      - *Supply Chain partners*

INCIDENT RESPONSE (IR)

- *IR-6: INCIDENT REPORTING*
  - *Suspected incidents to the organizational incident response capability:*
    - *Immediately but not to exceed one (1) hour after discovery; and*
    - *Report incident information to organizational personnel with incident handling responsibilities, and if confirmed, notify the CSO, SIB Chief, or Interface Agency Official.*
- *IR-6(1): AUTOMATED REPORTING*
  - *Report incidents using automated mechanisms*
    - *Email*
    - *Websites (with automatic updates)*
- *IR-6(3): SUPPLY CHAIN COORDINATION*
  - *Provide incident information to the provider of the product*

INCIDENT RESPONSE (IR)

- *IR-7: INCIDENT RESPONSE ASSISTANCE*
  - *Provide an incident response support resource that offers advice and assistance to users of the system for the handling and reporting of incidents*
    - *Help Desks*
    - *Assistance Groups*
    - *Automated Ticketing Systems*
- *IR-7(1): AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT*
  - *Increase the availability of incident response information and support using automated mechanisms*
    - *Push/pull capability to get assistance on incident*
    - *If external assistance (unescorted access to unencrypted CJI)*
      - *Security Addendum/Outsourcing Standard*

INCIDENT RESPONSE (IR)

- *IR-8: INCIDENT RESPONSE PLAN*
  - *Develop a plan that:*
    - *Provides roadmap for implementing incident response capability*
    - *Describes the structure and organization of the incident response capability*
    - *Provides a high-level approach for how the incident response capability fits into the overall organization*
    - *Meets organizations mission, size, structure, and functions*
    - *Defines reportable incidents*
    - *Provides metrics for measuring the incident response capability*
    - *Defines the resources and management support needed to effectively maintain and mature an incident response capability*
    - *Addresses the sharing of incident information*
    - *Reviewed and approved by the organization's/agency's executive leadership annually; and*
    - *Explicitly designates responsibility for incident response to organizational personnel with incident reporting responsibilities and CSO, SIB Chief, or Interface Agency Official.*

INCIDENT RESPONSE (IR)

- *IR-8: INCIDENT RESPONSE PLAN*
  - *Distribute copies of the incident response plan to organizational personnel with incident handling responsibilities,*
  - *Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;*
  - *Communicate incident response plan changes to organizational personnel with incident handling responsibilities; and*
  - *Protect the incident response plan from unauthorized disclosure and modification.*

INCIDENT RESPONSE (IR)

- *IR-8(1): BREACHES*
  - *Include the following if PII breach:*
    - *Process to determine if notice to individuals or other organizations, including oversight organizations, is needed;*
    - *An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and*
    - *Identification of applicable privacy requirements.*

AUDIT & ACCOUNTABILITY (AU)

AUDIT & ACCOUNTABILITY (AU)

- *AU-1: POLICY and PROCEDURES*
  - *Review annually*
- *AU-2: EVENT LOGGING*
  - *Identify types of events the system is capable of logging*
  - *Coordinate event logging with other organizational entities*
  - *Specify*
    - *Successful and unsuccessful:*
      - *Log-on attempts*
      - *Attempts to use permissions on resources*
      - *Attempts to change passwords*
      - *Actions by privileged accounts*
      - *Attempts to access/modify/destroy the log file(s)*
  - *Provide rationale for selected event types*
  - *Review/update selected types annually*

AUDIT & ACCOUNTABILITY (AU)

- *AU-3: CONTENT of AUDIT RECORDS*
  - *What / when / where / source / outcome / identify*
- *AU-3(1): ADDITIONAL AUDIT INFORMATION*
  - *Audit records to contain additional information:*
    - *Session, connection, transaction, duration*
    - *Source / destination addresses*
    - *Object / filename accessed*
    - *Number of bytes sent / received*
    - *III identification:*
      - *Operator*
      - *Authorized receiving agency*
      - *Requestor*
      - *Secondary recipient*

AUDIT & ACCOUNTABILITY (AU)

- *AU-3(3): LIMIT PII ELEMENTS*
  - *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).*
- *AU-4: AUDIT LOG STORAGE CAPACITY*
  - *Enough capacity to meet retention requirements in AU-11*
- *AU-5: RESPONSE TO AUDIT LOGGING PROCESS FAILURES*
  - *Alert within one (1) hour of failure*
  - *Restart logging and verify system(s) properly logging*

AUDIT & ACCOUNTABILITY (AU)

- *AU-6: AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING*
  - *Review and analyze weekly / report findings / adjust based on risk factors*
- *AU-6(1): AUTOMATED PROCESS INTEGRATION*
  - *Use automated mechanisms to review, analyze and report*
- *AU-6(3): CORRELATE AUDIT RECORD REPOSITORIES*
  - *Organization-wide situational awareness*

AUDIT & ACCOUNTABILITY (AU)

- *AU-7: AUDIT RECORD REDUCTION AND REPORT GENERATION*
  - *Capabilities that:*
    - *Support on-demand review / analysis / reporting / after-the-fact incident investigation*
    - *Does not alter original content*

- *AU-7(1): AUTOMATIC PROCESSING*
  - *Process / sort / search records of interest (collected in AU-3)*

AUDIT & ACCOUNTABILITY (AU)

- *AU-8: TIME STAMPS*
  - *Internal system clocks*
  - *UTC / fixed local offset from UTC / local time offset*
- *AU-9: PROTECTION OF AUDIT INFORMATION*
  - *Protect audit info and tools from unauthorized access / modification / deletion*
  - *Alert upon detection*
- *AU-9(1): ACCESS BY SUBSET OF PRIVILEGED USERS*
  - *Authorize access to only organizational personnel:*
    - *Audit and accountability*
    - *Information security and privacy*
    - *System/network administrators*

AUDIT & ACCOUNTABILITY (AU)

- *AU-11: AUDIT RECORD RETENTION*
  - *Minimum one (1) year or until no longer required*
- *AU-12: AUDIT RECORD GENERATION*
  - *Tailor log generation on systems required to log using content requirements in AU-2 and AU-3*

ACCESS CONTROL (AC)

ACCESS CONTROL (AC)

- *AC-1: POLICY and PROCEDURES*
  - *Review annually*
- *AC-2: ACCOUNT MANAGEMENT*
  - *Define types of accounts allowed and prohibited*
  - *Assign account managers*
  - *Require conditions for group/role membership*
  - *Specify*
    - *Authorized Users*
    - *Group/role membership*
    - *Access Authorizations/attributes for each account*
      - *Privileges*

AC-2 (D)(3): ACCESS AUTHORIZATIONS

- *Email Address Text*
- *Employer Name*
- *Federation Id*
- *Given Name*
- *Identity Provider Id*
- *Sur Name*
- *Telephone Number*
- *Identity Provider Id*
- *Unique Subject Id*
- *Counter Terrorism Data Self Search Home Privilege Indicator*
- *Criminal History Data Self Search Home Privilege Indicator*
- *Criminal Intelligence Data Self Search Home Privilege Indicator*
- *Criminal Investigative Data Self Search Home Privilege Indicator*
- *Display Name*
- *Government Data Self Search Home Privilege Indicator*
- *Local Id*
- *NCIC Certification Indicator*
- *N-DEx Privilege Indicator*
- *PCII Certification Indicator*
- *28 CFR Certification Indicator*
- *Employer ORI*
- *Employer Organization General Category Code*
- *Employer State Code*
- *Public Safety Officer Indicator*
- *Sworn Law Enforcement Officer Indicator*
- *Authenticator Assurance Level*
- *Federation Assurance Level*
- *Identity Assurance Level*
- *Intelligence Analyst Indicator*

ACCESS CONTROL (AC)

- *AC-2: ACCOUNT MANAGEMENT cont'd*
  - *Require approvals*
  - *Create, enable, modify, disable, and remove (Agency Policy)*
  - *Monitor the use*
  - *Notify account manager/system or network admins*
    - *One day:*
      - *Account no longer required*
      - *User transferred/terminated*
      - *Need to know changes*
  - *Authorize Access*
    - *Valid access*
    - *Intended system usage*
    - *Attributes*

ACCESS CONTROL (AC)

- *AC-2: ACCOUNT MANAGEMENT cont'd*
  - *Review accounts annually*
  - ***IF*** *using groups accounts; process when someone is removed?*
  - *Align processes with personnel termination/transfer process*
- *AC-2(1): AUTOMATED SYSTEM ACCOUNT MANAGEMENT*
  - *Email*
  - *Phone*
  - *Text*
- *AC-2(2): AUTOMATED TEMPORARY/EMERGENCY ACCOUNT*
  - *Remove within 72 hours*

ACCESS CONTROL (AC)

- *AC-2(3): DISABLE ACCOUNTS*
  - *Within (1) week when accounts:*
    - *Have expired*
    - *No longer associated with user*
    - *Violation of organizational policy, or*
    - *Inactive for 90 days*
- *AC-2(4): AUTOMATED AUDIT ACTIONS*
  - *Automatically audit account creation, modification, enabling, disabling, and removal actions*
- *AC-2(5): INACTIVITY LOGOUT*
  - *Require user log out when work period is complete*
- *AC-2(13): DISABLE ACCOUNTS FOR HIGH RISK*
  - *Direct threats to confidentiality, integrity, or availability*
  - *Within 30 minutes of discovery*

ACCESS CONTROL (AC)

- *AC-3: ACCESS ENFORCEMENT*
  - *Enforce approved authorizations for logical access*
- *AC-3(14): INDIVIDUAL ACCESS*
  - *Enable individuals to have access to elements of their PII*
- *AC-4: INFORMATION FLOW ENFORCEMENT*
  - *Control the flow of information*
    - *No unencrypted CJI across public network*
    - *Block outside traffic appearing from inside*
    - *Web requests from agency-controlled or internal boundary protection devices*
      - *Web proxy*
      - *Gateway*
      - *Firewalls*
      - *Routers*

ACCESS CONTROL (AC)

- *AC-5: SEPARATION OF DUTIES*
  - *Identify and document duties*
  - *Define system authorizations to support*
- *AC-6: LEAST PRIVILEGE*
  - *Just enough permission to complete mission*
- *AC-6(1): AUTHORIZE ACCESS TO SECURITY FUNCTIONS*
  - *Authorize access to privileged users:*
    - *Establish system accounts, configure access authorizations, event auditing, intrusion detection parameters, etc*
    - *Security relevant information in hardware, software, firmware*

ACCESS CONTROL (AC)

- *AC-6(2): NON-PRIVILEDGED ACCESS FOR NONSECURITY FUNCTIONS*
  - *Use appropriate role/credential for correct use*
- *AC-6(5): PRIVILEGED ACCOUNTS*
  - *Restrict privileged accounts to privileged users*
- *AC-6(7): REVIEW OF USER PRIVILEGES*
  - *Annually; reassign or remove to correctly reflect organizational needs*
- *AC-6(9): LOG USE OF PRIVILEGED FUNCTIONS*
  - *Log the execution of privileged functions*

ACCESS CONTROL (AC)

- *AC-6(10): PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*
  - *Non –privileged users do not possess appropriate authorizations*
- *AC-7: UNSUCCESSFUL LOGON ATTEMPTS*
  - *Limit of (5) five during a 15-minute time period*
  - *Automatically lock the account; admin must release*

ACCESS CONTROL (AC)

- *AC-8: SYSTEM USE NOTIFICATION*
  - *Before granting access*
    - *Accessing restricted information system*
    - *Usage may be monitored, recorded, subject to audit*
    - *Unauthorized use of the system is prohibited*
    - *Use of systems indicates consent*
  - *Retain the message of banner until user takes explicit action*
    - *Acknowledgment*
  - *For publicly accessible systems*
    - *Display system use information*
    - *Display references to monitoring, recording*
    - *Description of authorized uses of system*

ACCESS CONTROL (AC)

- *AC-11: DEVICE LOCK*
  - *Prevent further access after 30 minutes of inactivity*
  - *Require user to initiate before leaving system unattended*
  - *Retain device lock until user reestablishes access using I&A*
- *****EXEMPTION******
  - *In the interest of safety, devices that are:*
    - *(1) part of a criminal justice conveyance; or*
    - *(2) used to perform dispatch functions and located within a physically secure location; or*
    - *(3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement*

ACCESS CONTROL (AC)

- *AC-11(1): PATTERN-HIDING DISPLAYS*
  - *Conceal, via the device lock, information previously visible on the display with a publicly viewable image.*
- *AC-12: SESSION TERMINATION*
  - *Automatically terminate a user session after a user has been logged out*
- *AC-14: PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION*
  - *Identify, and document, specific user action that do not require I&A*

ACCESS CONTROL (AC)

- *AC-17: REMOTE ACCESS*
  - *Establish/document for each type of access:*
    - *Usage restrictions*
    - *Configuration/connection requirements*
    - *Implementation guidance*
  - *Authorize each type prior to allowing*
- *AC-17(1): MONITORING AND CONTROL*
  - *Use automation to monitor and control remote access*
- *AC-17(2): PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION*
  - *Use Virtual Private Networks (VPNs)*
  - *Transport Layer Security*
- *AC-17(3): MANAGED ACCESS CONTROL POINTS*
  - *Route remote accesses through authorized and managed access control points.*

ACCESS CONTROL (AC)

- *AC-17(4): PRIVILEGED COMMANDS AND ACCESS*
  - *Authorize only for compelling needs and document the rationale in the system security plan.*
- *AC-18: WIRELESS ACCESS*
  - *Establish configuration, connection requirements and implementation guidelines for each type of wireless access*
  - *Authorize each type of wireless access*
- *AC-18(1): AUTHENTICATION AND ENCRYPTION*
  - *Authenticate authorized users and agency devices*
  - *Encryption*
- *AC-18(3): DISABLE WIRELSS NETWORKING*
  - *If not using wireless networking capabilities, disable them*

ACCESS CONTROL (AC)

- *AC-19: ACCESS CONTROL FOR MOBILE DEVICES*
  - *Establish configuration and connection requirements and implementation guidance*
    - *Especially outside of controlled areas*
  - *Authorize connection of mobile devices*
- *AC-19(5): FULL DEVICE ENCRYPTION*
  - *Employ full device encryption to protect confidentiality and integrity*
- *AC-20: USE OF EXTERNAL SYSTEMS*
  - *Establish policies governing the use of external systems, OR*
  - *Prohibit the use of BYOD*

ACCESS CONTROL (AC)

- *AC-20(1): LIMITS ON AUTHORIZED USE*
  - *Permit authorized individuals to use external system after:*
    - *Verifying the controls on the external system, OR*
    - *Retention of processing agreements with the entity hosting external system*
- *AC-20(2): PORTABLE STORAGE DEVICES – RESTRICTED USE*
  - *Restrict your controlled portable storage devices on external systems.*
- *AC-21: INFORMATION SHARING*
  - *When sharing, ensure system is secure for CJI*
  - *Use ABAC to assist in securing*

ACCESS CONTROL (AC)

- *AC-22: PUBLICLY ACCESSIBLE CONTENT*
  - *Designate individuals authorized to make information publicly accessible;*
  - *Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;*
  - *Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and*
  - *Review the content on the publicly accessible system for nonpublic information quarterly and remove such information, if discovered.*

IDENTIFICATION & AUTHENTICATION (IA)

IDENTIFICATION AND AUTHENTICATION (IA)

- *IA-1: POLICY and PROCEDURES*
- 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.*

IDENTIFICATION AND AUTHENTICATION (IA)

- *IA-2(8): IA (Replay Resistant): Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.*
- *IA-2(12): IA (PIV Credentials): Accept and electronically verify Personal Identity Verification-compliant credentials*
- *IA-3: DEVICE IDENTIFICATION AND AUTHENTICATION*
  - *Uniquely identify and authenticate agency devices before establishing all remote and network connections. In the instance of local connection, the device must be approved by the agency and the device must be identified and authenticated prior to connection to an agency asset*

IDENTIFICATION AND AUTHENTICATION (IA)

- IA-4: IDENTIFIER MANAGEMENT
  - Receiving authorization from organizational personnel with identifier management responsibilities to assign an individual, group, role, service, or device identifier
  - Selecting an identifier that identifies an individual, group, role, service, or device;
  - Assigning the identifier to the intended individual, group, role, service, or device; and
  - *Preventing reuse of identifiers for one (1) year.*

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*

IDENTIFICATION AND AUTHENTICATION (IA)

- IA-5: AUTHENTICATOR MANAGEMENT cont’d
  - *Authenticator Types*
    - Memorized Secret (PW/PIN)
      - *Complex PW (October 1, 2024)*
      - Maintain list of compromised passwords
      - *Allow long passwords and passphrases*
      - *No truncation; no hints*
      - *Salt/hash memorized secret before storing*
    - Look Up Secrets
      - *20 bits of entropy*
      - *Bingo card; each grid shall only be used once; unattractive*
    - *Out of Band*
      - Separate Channel
      - *Must prove possession*
      - 10 minutes expiration
      - One time use

IDENTIFICATION AND AUTHENTICATION (IA)

- IA-5: AUTHENTICATOR MANAGEMENT cont'd
  - *Authenticator Types cont'd*
    - One Time Passcode
      - Six Digits
      - *Nonce change @ least every 2 minutes*
      - *Defined lifetime*
        - *30 seconds either side for clock drift*
    - *Cryptographic Authenticators*
      - *Software based?*
        - *Suitable storage area (TEE/TPM)*
        - *Cannot be removed from device*
      - *Hardware based?*
        - *Secret key and algorithm = 112 bits*
        - *Nonce = 64 bits of entropy*

IDENTIFICATION AND AUTHENTICATION (IA)

- IA-5(2): PUBLIC KEY-BASED AUTHENTICATION
  - Enforce authorized access to private key
  - Map authenticated identity to the account
  - Public key infrastructure
    - Validate certificates to the trusted anchor
      - Check certificate status
      - Local cache of revocation data
- IA-5(6): PROTECTION OF AUTHENTICATORS
  - Commensurate with the security categorization
    - CJI = MODERATE
- IA-6: AUTHENTICATION FEEDBACK
  - Obscure feedback

IDENTIFICATION AND AUTHENTICATION (IA)

- IA-7: CRYPTOGRAHIC MODULE AUTHENTICATION
  - Implement mechanisms for authentication to a cryptographic module that meet the requirements
- IA-8: IA (Non-ORGANIZATIONAL USERS)
  - Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.
- IA-8(1): EXTERNAL PIV CREDENTIALS
  - Accept and electronically verify Personal Identity Verification-compliant credentials from other federal, state, local, tribal, or territorial (SLTT) agencies.
- IA-8(2): ACCEPTANCE OF EXTERNAL AUTHENTICATORS
  - Accept only external authenticators that are NIST-compliant
  - Document and maintain a list of accepted external authenticators.

IDENTIFICATION AND AUTHENTICATION (IA)

- *IA-8(4): USE OF DEFINED PROFILES*
  - *Conform to the following profiles for identity management: Security Assertion Markup Language (SAML) or OpenID Connect.*
- *IA-11: RE-AUTHENTICATION*
  - *Require users to re-authenticate when:*
    - *roles, authenticators, or credentials change;*
    - *security categories of systems change;*
    - *the execution of privileged functions occur;*
    - *or every 12 hours.*

IDENTIFICATION AND AUTHENTICATION (IA)

- *IA-12: IDENTITY PROOFING*
  - *Resolve user identities to a unique individual; and*
  - *Collect, validate, and verify identity evidence*
- *IA-12(2): IDENTITY EVIDENCE*
  - *Require evidence of individual identification be presented to the registration authority*

IDENTIFICATION AND AUTHENTICATION (IA)

- *IA-12(3): IDENTITY EVIDENCE VALIDATION AND VERIFICATION*
  - *Agency defined resolution, validation, and verification methods*
  - *SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits*
  - *Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context*
  - *The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing*
    - *Voluntary*
    - *Mandatory*
    - *Consequences for not providing the attributes*

IDENTIFICATION AND AUTHENTICATION (IA)

- *IA-12(3): IDENTITY EVIDENCE VALIDATION AND VERIFICATION*
  - *Provide mechanisms for redress of applicant complaints or problems arising from the identity proofing*
  - *Maintain a record, including audit logs, of all steps taken to verify the identity of the applicant as long as the identity exists in the information system*
  - *Record the types of identity evidence presented in the proofing process*
  - *An enrollment code SHALL be comprised of one of the following*
    - *Random six character alphanumeric*
    - *A machine-readable optical label, such as a QR Code, that contains data of similar entropy*

IDENTIFICATION AND AUTHENTICATION (IA)

- *IA-12(3): IDENTITY EVIDENCE VALIDATION AND VERIFICATION*
  - *IDENTITY EVIDENCE*
    - *(1) SUPERIOR or*
    - *(1) STRONG+*
      - *If evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source*
      - *OR*
    - *(2) STRONG*
      - *OR*
    - *(1) STRONG, plus (2) FAIR*

IDENTIFICATION AND AUTHENTICATION (IA)

- *IA-12(3): IDENTITY EVIDENCE VALIDATION AND VERIFICATION*
  - *SUPERIOR Evidence*
    - *U.S. Passport*
    - *Personal Identity Verification (PIV) Card*
    - *Common Access Card (CAC)*
    - *Personal Identity Verification Interoperable (PIV-I) Card*
    - *Transportation Worker Identification Card (TWIC)*
    - *Native American Enhanced Tribal Card*
  - *STRONG+ Evidence*
    - *REAL ID*
    - *Enhanced ID Cards*
    - *U.S. Military Badge*

IDENTIFICATION AND AUTHENTICATION (IA)

- *IA-12(3): IDENTITY EVIDENCE VALIDATION AND VERIFICATION*
  - *STRONG Evidence*
    - *Native American Tribal Photo Identification Card*
    - *Driver's License or ID card (REAL ID noncompliant)*
  - *FAIR Evidence*
    - *School ID card*
    - *Utility account statement*
    - *Credit/debit card and account statement*
    - *Financial institution account statement*
  - *WEAK Evidence*
    - *US Social Security Card*
    - *Original or certified copy of a birth certificate*

IDENTIFICATION AND AUTHENTICATION (IA)

- *IA-12(5): ADDRESS CONFIRMATION*
  - *Registration code or notice of proofing be delivered through an out-of-band channel to the users address (physical or digital) of record.*
    - *Physical - Postal Address*
    - *Digital - Email Address/Telephone Number*
  - *Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation.*
  - *Enrollment Code Time-To-Live*
    - *10 days – Postal Address Contiguous US*
    - *30 days – Postal Address Outside of US*
    - *10 minutes – Telephone*
    - *24 hours – Email Address*

CONFIGURATION MANAGEMENT (5.7)

Section 5.7

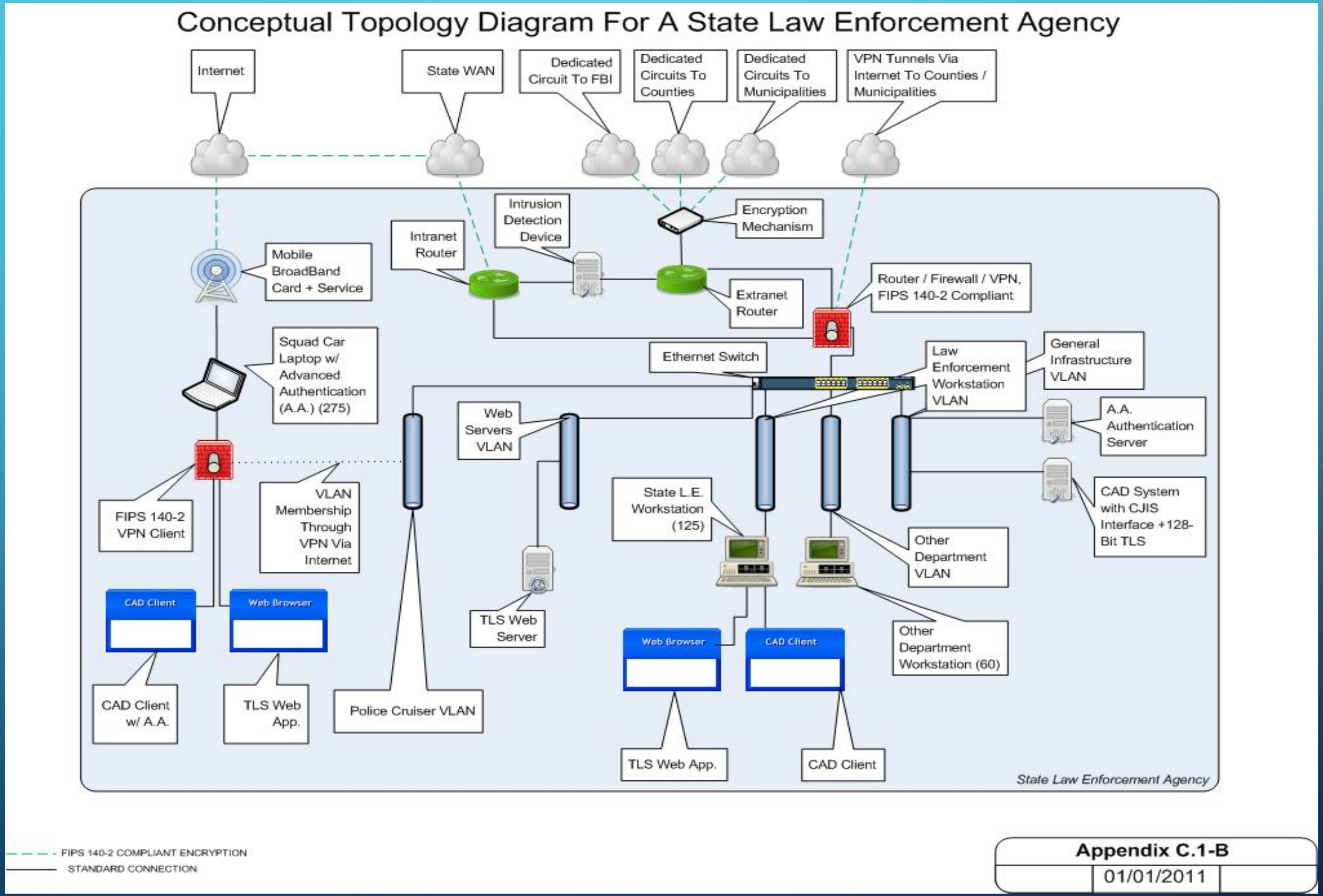
Policy Area 7: Configuration Management

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, Describes Agency Requirements for Control of Privileges and Restrictions*)

- **Least Functionality –** Configure Systems to Provide Only Essential Capabilities & Prohibit Use of Specified Services
- **Network Diagram –** Current, Complete Topological Drawing of Interconnectivity of CJIS Network and Services
- **Security of Configuration Documentation –** Protect System Documentation Consistent with Policy Area 5

Section 5.7

Policy Area 7: Configuration Management


Conceptual Topology Diagram For A State Law Enforcement Agency
Internet
State WAN
Dedicated Circuit To FBI
Dedicated Circuits To Counties
Dedicated Circuits To Municipalities
VPN Tunnels Via Internet To Counties / Municipalities
Intrusion Detection Device
Encryption Mechanism
Intranet Router
Mobile BroadBand Card + Service
Extranet Router
Router / Firewall / VPN, FIPS 140-2 Compliant
Squad Car Laptop w/ Advanced Authentication (A.A.) (275)
Ethernet Switch
Law Enforcement Workstation VLAN
General Infrastructure VLAN
Web Servers VLAN
A.A. Authentication Server
VLAN Membership Through VPN Via Internet
FIPS 140-2 VPN Client
State L.E. Workstation (125)
CAD System with CJIS Interface +128-Bit TLS
Other Department VLAN
CAD Client
Web Browser
TLS Web Server
Other Department Workstation (60)
CAD Client w/ A.A.
TLS Web App.
Police Cruiser VLAN
Web Browser
CAD Client
TLS Web App.
CAD Client
State Law Enforcement Agency
FIPS 140-2 COMPLIANT ENCRYPTION
STANDARD CONNECTION
Appendix C.1-B
01/01/2011

MEDIA PROTECTION (MP)

MEDIA PROTECTION (MP)

- *MP-1: POLICY and PROCEDURES*
  - *Review annually*
- *MP-2: MEDIA ACCESS*
  - *Restrict access to digital and non-digital media to authorized individuals*
- *MP-3: MEDIA MARKING**
  - *Mark media*
  - *Exempt digital & non-digital media marking within physically secure locations and controlled areas*

  - **MP-3 is currently exempted from audit*

MEDIA PROTECTION (MP)

- *MP-4: MEDIA STORAGE*
  - *Physically control and store digital and non-digital media in physically secure locations or controlled areas*
  - *Encrypt CJI on digital when physical or personnel restrictions not feasible*
  - *Protect until destroyed or sanitized*
- *MP-5: MEDIA TRANSPORT*
  - *Protect and control outside physically secure locations and controlled areas*
  - *Protect physical media commensurate with electronic*
  - *Restrict to authorized personnel*
  - *Maintain accountability outside physically secure locations and controlled areas*
  - *Document transport activities*
  - *Restrict activities to authorized personnel*

MEDIA PROTECTION (MP)

- *MP-6: MEDIA SANITIZATION*
  - *Sanitize or destroy digital and non-digital media:*
    - *Prior to disposal or release from agency control*
    - *Release for reuse using:*
      - *Overwrite technology (3 times)*
      - *Degaussing*
    - *Destroy inoperable digital media*
    - *Destroy physical media when no longer needed*
  - *Use sanitization methods commensurate with security category of information*

MEDIA PROTECTION (MP)

- *MP-7: MEDIA USE*
  - *Restrict use of media on agency owned systems (see examples)*
  - *Prohibit the use of personally owned media*
  - *Prohibit the use of digital media with no identifiable owner*
  - *EXAMPLES:*
    - *Technical controls: port disabling, access control lists (ACL), security groups, group policy objects (GPO), mobile device management (MDM).*
    - *Physical control: locked server cage, disconnect CD-ROM drive in PC, remove USB port.*
    - *Administrative controls: the agency's electronic media policy defining how flash drives are to be used within the agency rules of behavior.*

PHYSICAL & ENVIRONMENTAL PROTECTION (PE)

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

- *PE-1: POLICY AND PROCEDURES*
  - *Annual review*

- *PE-2: PHYSICAL ACCESS AUTHORIZATIONS*
  - *List of individuals with authorized facility access / review annually and on personnel changes / remove individuals when no longer require access / issue authorization credentials for access*

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

- *PE-3: PHYSICAL ACCESS CONTROL*
  - *Enforce physical access authorizations*
    - *Verify individual access authorizations*
    - *Control ingress/egress*
  - *Maintain physical access audit logs*
  - *Control access to non-public areas*
  - *Escort visitors and control visitor activity*
  - *Secure keys / combinations / physical access devices*
  - *Inventory agency-issued physical access devices annually*
  - *Change combinations / keys when lost / compromised / personnel transfer / termination*
  - *If unable to meet above, refer to PE-17 Alternate Work Site*

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

- *PE-4: ACCESS CONTROL FOR TRANSMISSION*
  - *Control physical access to distribution/transmission lines and devices*
- *PE-5: ACCESS CONTROL FOR OUTPUT DEVICES*
  - *Control physical access to output from monitors, printers, scanners, audio devices, facsimile machines, and copiers*
- *PE-6: MONITOR PHYSICAL ACCESS*
  - *Monitor physical access / detect & respond to physical security incidents / review logs quarterly*
- *PE-6(1): INTRUSION ALARMS AND SURVEILLANCE*
  - *Monitor physical access using physical intrusion alarms and surveillance equipment*

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

- PE-8: VISITOR ACCESS RECORDS
  - One (1) year / quarterly review / report anomalies
- PE-8(1): LIMIT PII
  - Limit PII to the minimum necessary for the purpose
- * PE-9 THROUGH PE-15 APPLY TO DATACENTERS AS DEFINED IN APPENDIX A
- PE-9: POWER EQUIPMENT AND CABLING
  - Protect power equipment and cabling from danger and destruction

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

- *PE-10: EMERGENCY SHUTOFF*
  - *Provide power shutoff capability for emergencies*
  - *Make emergency shutoff switches easily accessible*
  - *Protect switches from unauthorized activation*
- *PE-11: EMERGENCY POWER*
  - *Provide uninterruptable power for orderly shutdown*
- *PE-12: EMERGENCY LIGHTING*
  - *Employ and maintain emergency lighting*

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

- *PE-13: FIRE PROTECTION*
  - *Employ and maintain fire detection and suppression systems*
- *PE-13(1): AUTOMATIC ACTIVATION AND NOTIFICATION*
  - *Fire detection system that activates automatically and notifies emergency personnel*
- *PE-14: ENVIRONMENTAL CONTROLS*
  - *Maintain and monitor HVAC levels with the facility where the system resides*
- *PE-15: WATER DAMAGE PROTECTION*
  - *Protect system from water damage using shutoff/isolation valves*

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

- *PE-16: DELIVERY AND REMOVAL*
  - *Authorize and control system-related components entering/exiting the facility / maintain records*
- *PE-17: ALTERNATE WORK SITE*
  - *Determine/document allowable alternate facilities/locations*
  - *"Controlled Area"*
  - *Assess control effectiveness at alternate sites*
  - *Provide means for communication in case of incidents*

SYSTEMS & COMMUNICATIONS PROTECTION (SC)

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

- *SC-1: POLICY AND PROCEDURES*
  - *Annual review*
- *SC-2: SEPARATION OF SYSTEM AND USER FUNCTIONALITY*
  - *Separate user functionality from system management functionality*
- *SC-4: INFORMATION IN SHARED SYSTEM RESOURCES*
  - *Prevent unauthorized and unintended information transfer via shared system resources*

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

- *SC-5: DENIAL OF SERVICE PROTECTION*
  - *Protect against or limit the effects of denial-of-service type events using boundary protection devices and IDS/IPS*

- *SC-7: BOUNDARY PROTECTION*
  - *Monitor and control at external managed interfaces and key internal managed interfaces*
  - *Use physical or logical subnets for publicly accessible system components*
  - *Connect externally only through managed interfaces in accordance with organizational security and privacy architecture*

- *SC-7(3): ACCESS POINTS*
  - *Limit the number of external network connections*

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

- *SC-7(4): EXTERNAL TELECOMMUNICATIONS SERVICES*
  - *Managed interface for each external telecom service*
  - *Traffic flow policy for each managed interface*
  - *Protect information confidentiality and integrity across each interface*
  - *Document exceptions to traffic flow based on mission/business needs*
  - *Review exceptions annually, after incidents, after system changes, remove when no longer supported by mission/business need*
  - *Prevent unauthorized exchange of external control plane traffic*
  - *Detect unauthorized internal control plane traffic*
  - *Filter unauthorized external control plane traffic*

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

- *SC-7(5): DENY BY DEFAULT – ALLOW BY EXCEPTION*
  - *Deny by default – allow by exception*
- *SC-7(7): SPLIT TUNNELING FOR REMOTE DEVICES*
  - *Prevent split tunneling for remote devices connected to organizational system*
- *SC-7(8): ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*
  - *Route internal traffic to all untrusted networks through a proxy server*
- *SC-7(24): PERSONALLY IDENTIFIABLE INFORMATION*
  - *Apply processing rules to PII*
  - *Monitor for permitted processing at boundary and internally*
  - *Document processing exceptions / review and remove unsupported exceptions*

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

- *SC-8: TRANSMISSION CONFIDENTIALITY AND INTEGRITY*
  - *Protect the confidentiality and integrity of transmitted information / metadata from unencrypted CJI*
- *SC-8(1): CRYPTOGRAPHIC PROTECTION*
  - *Implement cryptographic mechanisms to prevent unauthorized disclosure and detect unauthorized changes or access*
- *SC-10: NETWORK DISCONNECT*
  - *Terminate network connection at end of session or after 1-hour of inactivity*
    - *Criminal justice conveyance*
    - *Dispatch inside a physically secure location*
    - *Receive only terminals (staffed physically secure location)*

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

- *SC-12: CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT*
  - *Establish and manage keys when cryptography is employed*

- *SC-13: CRYPTOGRAPHIC PROTECTION*
  - *Encryption for CJI in-transit*
  - *FIPS 140-3 certified or FIPS validated algorithm for symmetric key encryption/decryption (i.e., FIPS 197 AES)*
  - *NOTE: subsequent versions of approved modules under current review for FIPS 140-3 can be used until certification is complete. FIPS 140-2 certs not acceptable after Sept. 21, 2026.*

- *SC-15: COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS*
  - *Prohibit remote activation / notify users of use*

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

- *SC-17: PUBLIC KEY INFRASTRUCTURE CERTIFICATES*
  - *Issue certs under agency-level authority or obtain from an approved service provider*
  - *Only approved trust anchors (e.g., root certs) in agency-managed stores*

- *SC-18: MOBILE CODE*
  - *Define acceptable/unacceptable mobile code*
  - *Authorize / monitor /control mobile code use*

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

- *SC-20: SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)*
  - *Provide origin authentication and integrity verification along with authoritative name resolution*
  - *Provide means to indicate security status of child zones to enable verification of chain of trust*
- *SC-21: SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)*
  - *Request and perform authentication and verification on name/address responses from authoritative sources*

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

- *SC-22: ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE*
  - *Ensure fault-tolerance for systems providing name/address resolution*
  - *Implement internal and external role separation*

- *SC-23: SESSION AUTHENTICITY*
  - *Protect the authenticity of communications sessions*

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

- *SC-28: PROTECTION OF INFORMATION AT REST*
  - *Protect the confidentiality and integrity of CJI when outside a physically secure location using:*
    - *Cryptographic modules which are certified FIPS 140-3 with a symmetric128-bit cipher key OR*
    - *FIPS 197 with a symmetric 256-bit cipher key*
  - *Metadata from unencrypted CJI:*
    - *Protect as CJI*
    - *No use for advertising commercial purposes*
  - *Cloud storage of CJI:*
    - *Regardless of encryption status*
    - *APB-member country (U.S, U.S. territories, Indian Tribes, Canada)*

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

- *SC-28(1): CRYPTOGRAPHIC PROTECTION*
  - *Implement cryptographic protection of CJI at rest on information systems and digital media when outside a physically secure location*

- *SC-39: PROCESS ISOLATION*
  - *Separate execution domain for each executing system process*

FORMAL AUDITS (5.11)

Section 5.11

Policy Area 11: Formal Audits

Conducted to ensure compliance with applicable statutes, regulations, and policies

Audits by the FBI CJIS Division

- Triennial compliance audits
- Triennial security audits

Audits by the CSA

- Triennially audit all criminal justice with “direct access” to CJIS systems
- In coordination with the SIB, periodically audit all public and private NCJAs with access to CJI
- Authority for unannounced security inspections and scheduled audits of contractor facilities

PERSONNEL SECURITY (5.12)

Section 5.12

Policy Area 12: Personnel Security

Personnel Security

Having proper security measures in place to protect against an insider threat is a critical component for the CJIS Security Policy. The security terms and requirements of Section 5.12 apply to ALL personnel who have access to unencrypted CJI, including those individuals with physical access and/or logical access to devices that store, process, or transmit unencrypted CJI.

Personnel Security Policy and Procedures

The CSO, or their designee, is authorized to approve access to CJI. It is important to note that all CSO designees shall be from an authorized criminal justice agency. The decision shall be based off the results of the following checks:

- Appropriate background checks prior to access for all personnel with unescorted access to unencrypted CJI
- Reinvestigations are recommended for every five (5) years unless Rap Back is implemented

Section 5.12

Policy Area 12: Personnel Security

Personnel Termination

- Upon termination of individual employment, immediately terminate access to CJI.

Personnel Transfer

- The agency shall review the CJI access authorizations when personnel are reassigned or transferred to other positions.

Personnel Sanctions

- Employ a formal sanctions process for personnel failing to comply with policies and procedures.

MOBILE DEVICES (5.13)

Section 5.13

Policy Area 13: Mobile Devices

Wireless Communications Technology

- Wireless protocol considerations, cellular devices, Bluetooth, mobile hotspots.

Mobile Device Management (MDM)

- Access to CJI from mobile devices running a limited-feature OS.

Section 5.13

Policy Area 13: Mobile Devices

Wireless Device Risk Mitigations

- General requirements.

System Integrity

- Patching/updates, malicious code protection, personal firewall (full-featured OS devices).

Section 5.13
Policy Area 13: Mobile Devices

Incident Response

- In addition to 5.3, special reporting procedures for unique situations.

Access Control

- Rely on applications which access CJI.

Identification & Authentication

- Local device authentication, AA and compensating controls.

SYSTEM & SERVICES ACQUISITION (SA)

SYSTEM AND SERVICES ACQUISITION (SA)

- *SA-22: UNSUPPORTED SYSTEM COMPONENTS*
  - *Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or*
  - *Provide the following option for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support*

SYSTEM & INFORMATION INTEGRITY (SI)

SYSTEM AND INFORMATION INTEGRITY (SI)

- *SI-1: POLICY AND PROCEDURES*
- *SI-2: FLAW REMEDIATION*
  - *Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;*
  - *Install security-relevant software and firmware updates within the number of days listed after the release of the updates;*
    - *Critical – 15 days*
    - *High – 30 days*
    - *Medium – 60 days*
    - *Low – 90 days*
- *SI-2(2): 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

SYSTEM AND INFORMATION INTEGRITY (SI)

- *SI-3: MALICIOUS CODE PROTECTION*
  - Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code
  - *Automatically update malicious code protection mechanisms as new releases are available*
  - *Configure malicious code mechanisms*
    - 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
    - *Block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures; and send alert to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection*
  - *Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.*

SYSTEM AND INFORMATION INTEGRITY (SI)

- *SI-4: SYSTEM MONITORING*
  - *Monitor system to detect*
    - *Attacks and indicators of potential attacks in accordance with the following monitoring objectives*
      - *Intrusion detection and prevention*
      - *Malicious code protection*
      - *Vulnerability scanning*
      - *Audit record monitoring*
      - *Network monitoring*
      - *Firewall monitoring*
    - *Unauthorized local, network, and remote connections*
  - *Identify unauthorized use of the system through the following techniques and methods:*
    - *event logging (ref. 5.4 Audit and Accountability)*

SYSTEM AND INFORMATION INTEGRITY (SI)

- *SI-4: SYSTEM MONITORING con't*
  - *Invoke internal monitoring capabilities or deploy monitoring devices:*
    - *Strategically within the system to collect organization-determined essential information; and*
    - *At ad hoc locations within the system to track specific types of transactions of interest to the organization*
  - *Analyze detected events and anomalies*
  - *Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation*
  - *Obtain legal opinion regarding system monitoring activities; and*
  - *Provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs to organizational personnel with information security responsibilities weekly*

SYSTEM AND INFORMATION INTEGRITY (SI)

- SI-4(2): AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS
  - Employ automated tools and mechanisms to support near-real-time analysis of events
- SI-4(4): INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC
  - Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic
  - Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions such as: the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information

SYSTEM AND INFORMATION INTEGRITY (SI)

- SI-4(5): SYSTEM-GENERATED ALERTS
  - Alert organizational personnel with system monitoring responsibilities when the following system-generated indications of compromise or potential compromise occur: inappropriate or unusual activities with security or privacy implications
- SI-5: SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
  - Receive information system security alerts/, advisories, and directives from external source(s) (e.g., CISA, Multi-State Information Sharing & Analysis Center [MS-ISAC], U.S. Computer Emergency Readiness Team [USCERT], hardware/software providers, federal/state advisories, etc.) on an regular ongoing basis
  - Generate internal security alerts, advisories, and directives as deemed necessary
  - Issue Disseminate security alerts/, advisories, and directives to: organizational personnel implementing, operating, maintaining, and using the system appropriate personnel; and
  - *Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance*

SYSTEM AND INFORMATION INTEGRITY (SI)

- *SI-7: SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY*
  - Employ integrity verification tools to detect unauthorized changes to software, firmware, and information systems that contain or process CJI; and
  - Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate.
- *SI-7(1): INTEGRITY CHECKS*
  - *Perform an integrity check of software, firmware, and information systems that contain or process CJI at agency-defined transitional states or security relevant events at least weekly or in an automated fashion.*

SYSTEM AND INFORMATION INTEGRITY (SI)

- *SI-7(7): INTEGRATION OF DETECTION AND RESPONSE*
  - *Incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges.*
- SI-8: SPAM PROTECTION
  - Employ spam protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) to detect and act on unsolicited messages; and
  - Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

SYSTEM AND INFORMATION INTEGRITY (SI)

- *SI-8(2): AUTOMATIC UPDATES*
  - *Automatically update spam protection mechanisms at least daily*
- *SI-10: INFORMATION INPUT VALIDATION*
  - *Check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI*
- *SI-11: ERROR HANDLING*
  - *Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and*
  - *Reveal error messages only to organizational personnel with information security responsibilities*

SYSTEM AND INFORMATION INTEGRITY (SI)

- SI-12: INFORMATION MANAGEMENT AND RETENTION
  - Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements
- SI-12(1): LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS
  - Limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3)
- *SI-12(2): MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH*
  - *Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: data obfuscation, randomization, anonymization, or use of synthetic data*
- SI-12(3): INFORMATION DISPOSAL
  - Use the following techniques to dispose of, destroy, or erase information following the retention period: as defined in MP-6

SYSTEM AND INFORMATION INTEGRITY (SI)

- *SI-16: MEMORY PROTECTION*
  - *Implement the following controls to protect the system memory from unauthorized code execution: data execution prevention and address space layout randomization*

MAINTENANCE (MA)

MAINTENANCE (MA)

- *MA-1: POLICY and PROCEDURES*
  - *Review annually*
- *MA-2: CONTROLLED MAINTENANCE*
  - *Schedule, document, and review records of maintenance, repair, and replacement on system components*
  - *Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location.*
  - *Require that organizational personnel with information security and privacy responsibilities explicitly approve the removal of the system or system components*

MAINTENANCE (MA)

- MA-2: CONTROLLED MAINTENANCE
  - Sanitize equipment to remove information from associated media prior to removal from organizational facilities for off-site maintenance, repair, replacement, or destruction;
  - Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
  - Include the following information in organizational maintenance records:
    - Component name
    - Component serial number
    - Date/time of maintenance
    - Maintenance performed
    - Name(s) of entity performing maintenance including escort if required.

MAINTENANCE (MA)

- *MA-3: MAINTENANCE TOOLS*
  - *Approve, control, and monitor the use of system maintenance tools; and*
  - *Review previously approved system maintenance tools prior to each use.*
- *MA-3(1): INSPECT TOOLS*
  - *Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.*
- *MA-3(2): INSPECT MEDIA*
  - *Check media containing diagnostic and test programs for malicious code before the media are used in the system.*

MAINTENANCE (MA)

- *MA-3(3): PREVENT UNAUTHORIZED REMOVAL*
  - *Prevent the removal of maintenance equipment containing organizational information by:*
    - *Verifying that there is no organizational information contained on the equipment;*
    - *Sanitizing or destroying the equipment;*
    - *Retaining the equipment within the facility; or*
    - *Obtaining an exemption from organizational personnel with system maintenance responsibilities explicitly authorizing removal of the equipment from the facility*

MAINTENANCE (MA)

- *MA-4: NONLOCAL MAINTENANCE*
  - *Approve and monitor nonlocal maintenance and diagnostic activities;*
  - *Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;*
  - *Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;*
  - *Maintain records for nonlocal maintenance and diagnostic activities; and*
  - *Terminate session and network connections when nonlocal maintenance is completed*

MAINTENANCE (MA)

- *MA-5: MAINTENANCE PERSONNEL*
  - *Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;*
  - *Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and*
  - *Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations*

MAINTENANCE (MA)

- *MA-6: TIMELY MAINTENANCE*
  - *Obtain maintenance support and/or spare parts for critical system components that process, store, and transmit CJI within agency-defined recovery time and recovery point objectives of failure.*

PLANNING (PL)

PLANNING (PL)

- *PL-1: POLICY AND PROCEDURES*
  - *Annual review*
- *PL-2: SYSTEM SECURITY AND PRIVACY PLANS*
  - *Develop / Distribute / Coordinate / Review / Update / Communicate / Incorporate / PROTECT*

PLANNING (PL)

- *PL-4: RULES OF BEHAVIOR*
  - *Establish and provide to individuals with access rules that describe responsibility and expected behavior for use, security , and privacy*
  - *Documented acknowledgement prior to access*
  - *Review/update at least annually*
  - *Read and re-acknowledge by users when rules are revised or updated*
- *PL-4(1): SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS*
  - *Use of social media/sites, external sites/applications*
  - *Posting organizational info on public sites*
  - *Use of credentials for external site/application accounts*

PLANNING (PL)

- *PL-8: SECURITY AND PRIVACY ARCHITECTURES*
  - *Develop security and privacy architectures that:*
    - *Describe requirements and approach for protecting the "CIA" of organizational information and PII*
    - *Describe how they integrate into and support the enterprise architecture*
    - *Describe interaction with external systems/services*
  - *Review/update annually and on changes / integrate planned changes*

PLANNING (PL)

- *PL-9: CENTRAL MANAGEMENT*
  - *The CJISSECPOL is centrally managed by the FBI CJIS ISO*
- *PL-10: BASELINE SELECTION*
  - *Select a control baseline for the system*
- *PL-11: BASELINE TAILORING*
  - *Tailor the selected control baseline by applying specified tailoring actions*

CONTINGENCY PLANNING (CP)

CONTINGENCY PLANNING (CP)

- *CP-1: POLICY AND PROCEDURES*
  - *Annual review*
- CP-2: CONTINGENCY PLAN
  - *Develop / Distribute / Coordinate / Review / Update / Communicate / Incorporate / PROTECT*
- *CP-2(1): COORDINATE WITH RELATED PLANS*
  - *Biz continuity / DR / CIF / CONOPS / Crisis comms / IR / etc.*
- *CP-2(3): RESUME MISSION AND BUSINESS FUNCTIONS*
  - *Within 24 hours of plan activation*
- *CP-2(8): IDENTIFY CRITICAL ASSETS*
  - *Identify critical system assets supporting essential mission and business functions*

CONTINGENCY PLANNING (CP)

- *CP-3: CONTINGENCY TRAINING*
  - *Consistent with assigned roles / responsibilities*
    - *Within 30 days / System changes / Annually*
  - *Review/update annually / incidents / simulations or exercises*
- *CP-4: CONTINGENCY PLAN TESTING*
  - *Annually / review results / initiate corrective actions*
- *CP-4(1): COORDINATE WITH RELATED PLANS*
  - *Biz continuity / DR / CIF / CONOPS / Crisis comms / IR / etc.*

CONTINGENCY PLANNING (CP)

- *CP-6: ALTERNATE STORAGE SITE*
  - *Establish alternate storage site (system backup info) with agreements and controls equivalent to the primary site*
- *CP-6(1): SEPARATION FROM PRIMARY SITE*
  - *Sufficiently separated to reduce susceptibility to same threats*
- *CP-6(3): ACCESSIBILITY*
  - *Identify potential problems in event of an area-wide disruption and outline explicit mitigation actions*

CONTINGENCY PLANNING (CP)

- *CP-7: ALTERNATE PROCESSING SITE*
  - *Establish alternate processing site with equipment/supplies/ contracts in-place to resume operations, and controls equivalent to the primary site*
- *CP-7(1): SEPARATION FROM PRIMARY SITE*
  - *Sufficiently separated to reduce susceptibility to same threats*
- *CP-7(2): ACCESSIBILITY*
  - *Identify potential problems in event of an area-wide disruption and outline explicit mitigation actions*
- *CP-7(3): PRIORITY OF SERVICE*
  - *Develop agreements containing priority-of-service provisions to meet recovery time objectives*

CONTINGENCY PLANNING (CP)

- *CP-8: TELECOMMUNICATIONS SERVICES*
  - *Establish alternate telecommunications services*
- *CP-8(1): PRIORITY OF SERVICE PROVISIONS*
  - *Develop primary and alternate telecommunications service agreements*
  - *Request service priority or all telecommunications services for national security emergency preparedness*
- *CP-8(2): SINGLE POINTS OF FAILURE*
  - *Obtain alternate telecommunications services to reduce likelihood of sharing a single point of failure with primary telecommunications services*

CONTINGENCY PLANNING (CP)

- *CP-9: SYSTEM BACKUP*
  - *Back up user/system-level information & system documentation*
  - *Protect the confidentiality, integrity, & availability of backup info*
- *CP-9(1): TESTING FOR RELIABILITY AND INTEGRITY*
  - *Test as required by the contingency plan to verify reliability and integrity*
- *CP-9(2): CRYPTOGRAPHIC PROTECTION*
  - *Implement cryptographic mechanisms to prevent unauthorized disclosure/modification of CJI (SC-13 and/or SC-28)*

CONTINGENCY PLANNING (CP)

- *CP-10: SYSTEM RECOVERY AND RECONSTITUTION*
  - *Provide for recovery/reconstitution to a known state within timeframe required by contingency plan*
- *CP-10(2): TRANSACTION RECOVERY*
  - *Implement transaction recovery for transaction-based systems*

RISK ASSESSMENT (RA)

RISK ASSESSMENT (RA)

- *RA-1: POLICY AND PROCEDURES*
  - *Annual review*
- *RA-2: SECURITY CATEGORIZATION*
  - *The FBI CJIS Advisory Policy Board (APB) has assigned a security categorization of "moderate" for CJI and systems that process, store, and transmit CJI.*

RISK ASSESSMENT (RA)

- *RA-3: RISK ASSESSMENT*
  - *Conduct a risk assessment*
    - *Identify threats and vulnerabilities*
    - *Determine the likelihood and magnitude of harm*
    - *Determine the likelihood and impact for processing PII*
  - *Integrate mission and organization risk assessments and decisions with system-level assessments*
  - *Document assessments*
  - *Review risk assessment results at least quarterly*
  - *Disseminate assessment results to key personnel*
  - *Update the risk assessment at least quarterly or when changes to the system warrant*

RISK ASSESSMENT (RA)

- *RA-5: VULNERABILITY MONITORING AND SCANNING*
  - *Monitor and scan monthly and when new vulnerabilities are identified and reported*
  - *Employ vulnerability monitoring tools/techniques*
  - *Analyze vulnerability scanning and monitoring reports*
  - *Remediate vulnerabilities*
    - *Critical – 15 days*
    - *High – 30 days*
    - *Medium – 60 days*
    - *Low – 90 days*
  - *Share information from assessments with key personnel*
  - *Employ vulnerability monitoring tools that are readily updateable*

RISK ASSESSMENT (RA)

- *RA-5(2): UPDATE VULNERABILITIES TO BE SCANNED*
  - *Update within 24 hours prior to new scan or when new vulnerabilities are identified/reported*
- *RA-5(5): PRIVILEGED ACCESS*
  - *Implement privileged access for vulnerability scanning activities*
- *RA-5(11): PUBLIC DISCLOSURE PROGRAM*
  - *Establish a public reporting channel to receive reports of vulnerabilities*

RISK ASSESSMENT (RA)

- *RA-7: RISK RESPONSE*
    - *Respond to findings in accordance with organizational risk tolerance*
- *RA-9: CRITICALITY ANALYSIS*
    - *Identify critical system components and perform criticality analysis during the system development life cycle*

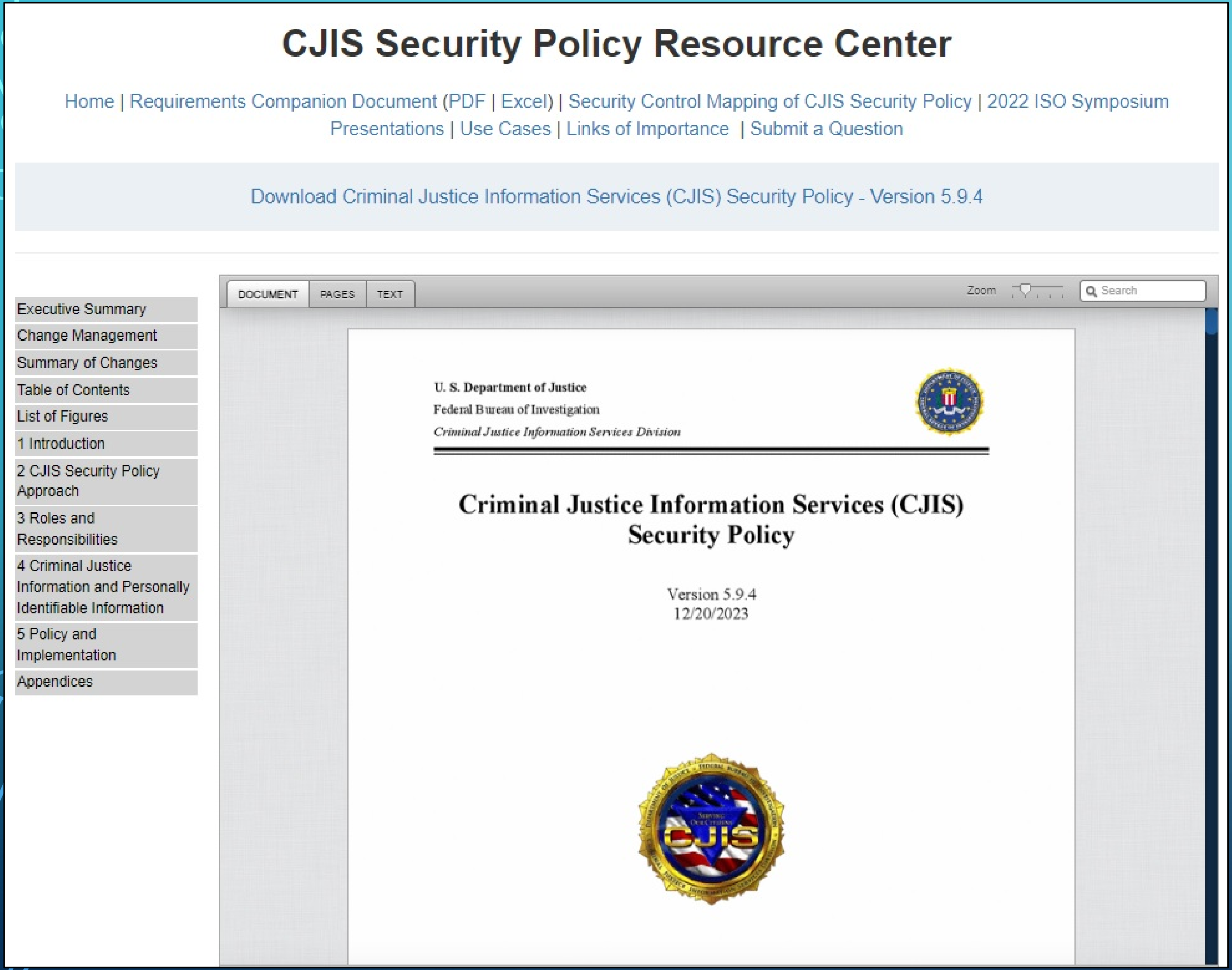
FBI CJIS ISO RESOURCES

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

iso@fbi.gov

CJISSECPOL Resource Center Website



CJIS Security Policy Resource Center

Home | Requirements Companion Document (PDF | Excel) | Security Control Mapping of CJIS Security Policy | 2022 ISO Symposium Presentations | Use Cases | Links of Importance | Submit a Question

Download Criminal Justice Information Services (CJIS) Security Policy - Version 5.9.4

- Executive Summary
- Change Management
- Summary of Changes
- Table of Contents
- List of Figures
- 1 Introduction
- 2 CJIS Security Policy Approach
- 3 Roles and Responsibilities
- 4 Criminal Justice Information and Personally Identifiable Information
- 5 Policy and Implementation
- Appendices

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

Criminal Justice Information Services (CJIS) Security Policy

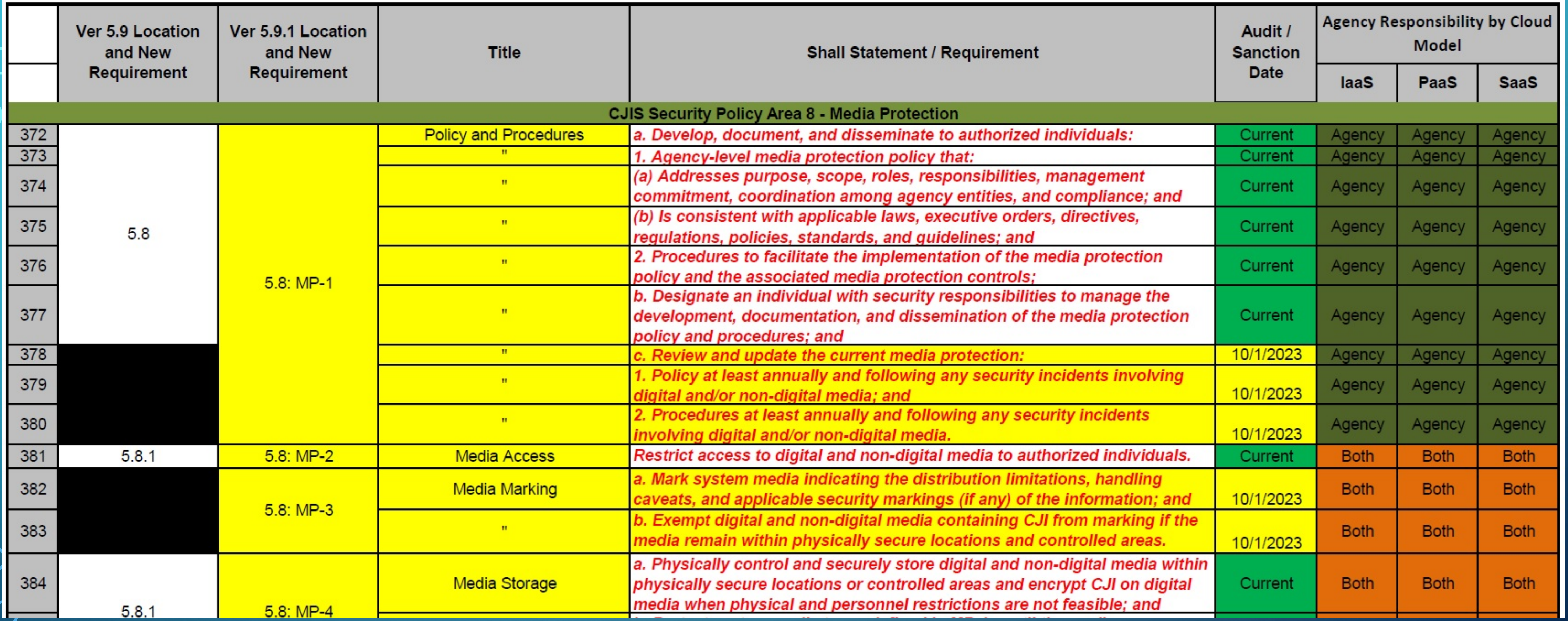
Version 5.9.4
12/20/2023

Requirements Companion document

- Companion document to the CJIS Security Policy
- Lists every requirement & “shall” statement, and corresponding location and effective date
- Lists the “Audit / Sanction” date for each requirement (modernization)
- 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 Location and New Requirement	Ver 5.9.1 Location and New Requirement	Title	Shall Statement / Requirement	Audit / Sanction Date	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
	CJIS Security Policy Area 8 - Media Protection							
372	5.8	5.8: MP-1	Policy and Procedures	*a. Develop, document, and disseminate to authorized individuals:*	Current	Agency	Agency	Agency
373			"	*1. Agency-level media protection policy that:*	Current	Agency	Agency	Agency
374			"	*(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and*	Current	Agency	Agency	Agency
375			"	*(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and*	Current	Agency	Agency	Agency
376			"	*2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;*	Current	Agency	Agency	Agency
377			"	*b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures; and*	Current	Agency	Agency	Agency
378			"	*c. Review and update the current media protection:*	10/1/2023	Agency	Agency	Agency
379			"	*1. Policy at least annually and following any security incidents involving digital and/or non-digital media; and*	10/1/2023	Agency	Agency	Agency
380			"	*2. Procedures at least annually and following any security incidents involving digital and/or non-digital media.*	10/1/2023	Agency	Agency	Agency
381	5.8.1	5.8: MP-2	Media Access	*Restrict access to digital and non-digital media to authorized individuals.*	Current	Both	Both	Both
382		5.8: MP-3	Media Marking	*a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and*	10/1/2023	Both	Both	Both
383			"	*b. Exempt digital and non-digital media containing CJI from marking if the media remain within physically secure locations and controlled areas.*	10/1/2023	Both	Both	Both
384	5.8.1	5.8: MP-4	Media Storage	*a. 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*	Current	Both	Both	Both

iso@fbi.gov

FBI CJIS ISO Contact Information

Chris Weatherly
FBI CJIS ISO

Jeff Campbell
FBI CJIS Deputy ISO

Holden Cross
Sr. Technical Analyst

iso@fbi.gov

Information Technology Security (ITS) Audit

Erica Anderson
Information Technology Specialist
Criminal Justice Information Services (CJIS)
Audit Unit (CAU)

Jeff Campbell
FBI CJIS Deputy ISO

Objectives

- Scope of the ITS audit
- Framework – *CJIS Security Policy*
- Process/Time Frame/Selection
- ITS Process

Scope

- Each automated program that CJIS offers has its own unique audit program, i.e. National Crime Information Center, Next Generation Identification, National Data Exchange System, etc.
- The ITS audit combines all those programs into one audit to ensure that all security risks and vulnerabilities have been identified that could affect CJIS system data.

Framework - *CJIS Security Policy*

- The Framework for all ITS Audits.
- The purpose of the *CJIS Security Policy* is to provide a minimum level of ITS requirements determined acceptable for the transmission, processing, and storage of CJIS data.
- The CJIS Systems Agency (CSA) can have more strict technical security guidelines.
- The *CJIS Security Policy (CSP)* is currently undergoing modernization. When modernization is complete, the result will be Version 6.0 of the *CSP*.

Shall Statements

- There are over 600 shall statements within the current *CJIS Security Policy*.
- Currently auditing to version 5.9.2.
- Shared management philosophy with FBI/CJIS and CSA.

Criminal Justice Information (CJI)

- Criminal Justice Information is the term used to refer to all of the FBI 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. Think of CJI as any record information that comes from the CJIS Division.

Process/Time Frame/Selection

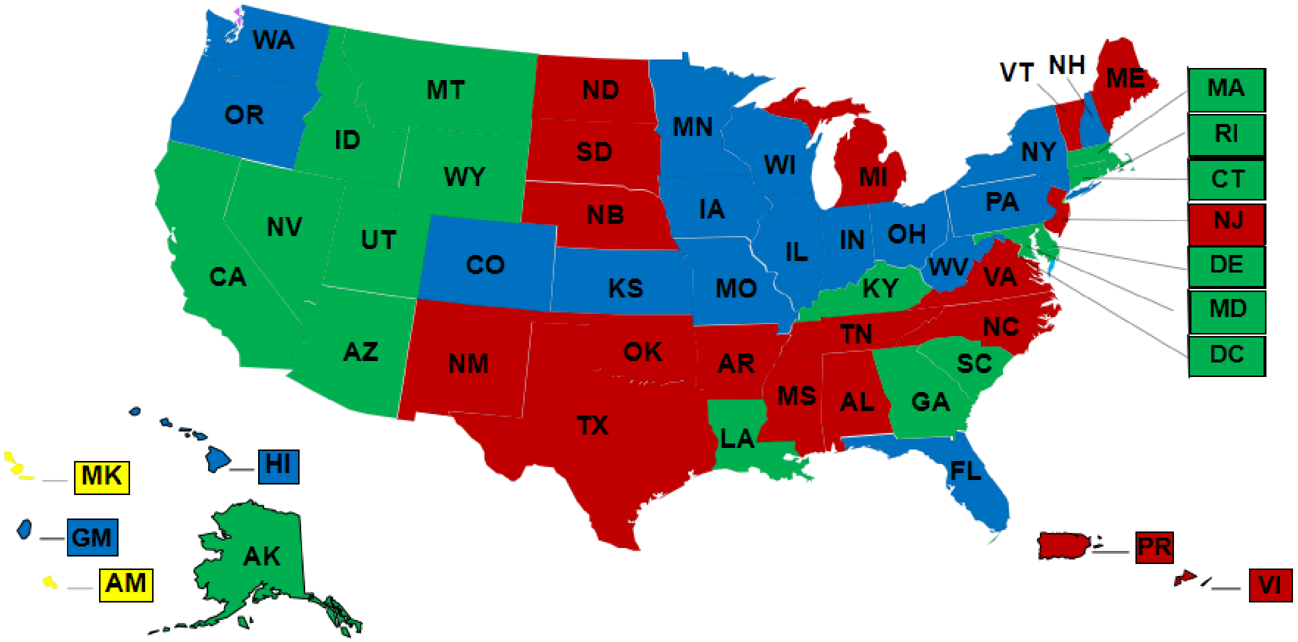
- CSA is notified approximately 6-9 months in advance that it will be audited in a particular month
- Initial contact call to CSA approximately 140 days prior to audit.
- Send pre-audit questionnaire
- Conduct audit by all audit programs, typically same week.
- ITS audit questionnaire
- Physical inspection
- Complete control assessment and leave with agency (draft)
- Compile audit report from CSA audit findings.

Process/Time Frame/Selection

- Audits are on a 3-year cycle.
- CSA is expected to visit all local agencies within a 3-year time frame.
- CAU only visits a small statistical sample of local agencies.
- Look for trends in the state and also nationally.
- ITS audit is approximately 2-3 hours.

3-year audit plan (Fiscal Year (FY)) is October 1st of previous year – September)

FY2024 FY2025 FY2026



ITS Audit Process – Onsite broken into two portions

- Administrative Review
  - Agency Coordinator
  - Management Control
  - Security Addendum
  - Personnel Security
  - Security Awareness Training
  - Walk through of agency
- Technical Review
  - User ID
  - Authentication
  - Advanced Authentication
  - Encryption

Administration of Criminal Justice Functions

- Administration of Criminal Justice:
  - Noncriminal Justice Governmental Agency (NCJGA)
  - Private Contractor (PC)

- Agreement/Contract:
  - NCJGA - Management Control Agreement
  - PC - Security Addendum and signature sheet

Personnel Security

- All unescorted personnel with unescorted access to criminal justice information have to be state and nationally fingerprinted.

Security Awareness Training

- Required topics are defined in policy
- Security Awareness Training is a different requirement from N-DEx policy training requirement
- 4 Tiered approach
- Limited – janitorial, clerical, and file
- Terminal – Terminal Access and Record Management Systems
- IT employees

Modernized Audit Plan

Day 1: CSA for Criminal and Non-Criminal audits (This can be extended to two days and have Criminal and Non-Criminal each have full days at the request of the CSA.)

Day 2: Local Criminal audits

Day 3: Local Non-Criminal audits

CSA selects the local agencies. We highly recommend someone from the CSA attending the local agency audits.

Modernized Reporting

1. Criminal justice report contains findings from the CSA.
2. Noncriminal justice report contains findings from the CSA or State Identification Bureau.

- The local agencies and the CJIS Security Officer's will be provided with a control assessment from the local audits, but if there were findings at the locals, it will not be included in the Sanctions report.

QUESTIONS

Please address questions and comments to:

Nick Cinalli
Supervisory IT Specialist
CJIS Audit Unit
(304) 625-3020
<cjisaudit@fbi.gov>

StateRAMP

StateRAMP
Third Party Risk Management for Public Sector

2024 FBI CJIS ISO Symposium

June 2024

Speakers

Chance Grubb

Government Engagement Director

chance@stateramp.org

www.stateramp.org

David Resler

Director, Information Security

david@stateramp.org

www.stateramp.org

Cloud Technology: Risks and Consequences

- CIS report showed significant increase in State & Local cyber events in 2023 over 8 months studied, compared to the same period in 2022

  - **148% more** malware attacks
  - **51% more** ransomware incidents
  - **313% increase** in data breaches and other endpoint compromises

- Rate of ransomware attacks on **K-12 providers reached 80% in 2023**, up from 56% the previous year, making it the highest of any industry

Disrupted services: School and office closures, inaccessible records, and compromised communication systems can significantly impact services at all levels of government.

Privacy concerns: Exposure of sensitive citizen data can have long-term consequences for identity theft and financial security.

Current State of Service Provider Risk Management

- Complex review process with diverse compliance frameworks, comparing apples to oranges, creates a business ‘unfriendly’ process
- Limited review, due to lack of bandwidth, leads to concerns about true security
- Self-attestation from service providers potentially leaves a wide security gap

> “*__50%__ of every industry surveyed stated that managing third-party security is overwhelming and a drain on internal resources*”

StateRAMP

StateRAMP is a non-profit, with members in the public and private sectors with a mission to promote best practices in cloud cybersecurity and a standardized approach to verifying cloud solutions.

Members leverage standardized assessments to verify cloud security.

Ongoing information sharing helps partners manage risk and continuously improve.

What is StateRAMP?

A step toward Framework Harmonization.

Based on NIST 800-53, StateRAMP has developed tiers of independently verifiable security certifications for service providers to achieve to demonstrate that they are meeting the requirements needed for the type of data they hold, process, and transmit.

StateRAMP was created as a public-private venture to bring public sector interests, industry interests, and auditor interests together to create a seamless process and platform to:

- Gain clear, ongoing insight into the cybersecurity posture of business partners
- Relieve burden on procurement and IT/Info Sec teams to review diverse compliance frameworks
- Advance risk management strategy further upstream

- Gain a verify once, serve many approach to compliance
- Demonstrate ‘trusted partner’ status
- Reduce barriers to competition through a comprehensive compliance framework

StateRAMP Program Benefits

Efficiency

Objective Standards

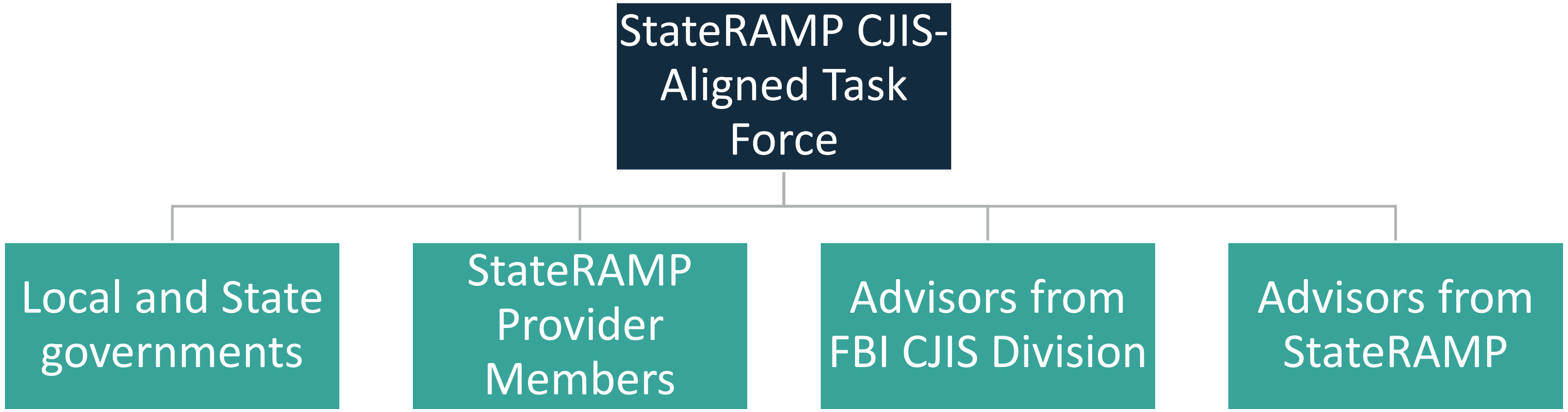
Cost Savings

Increased Competition

Improved Security

- Increase alignment between IT, InfoSec and Procurement
- Address workforce challenges by shifting personnel from “assessor” to “oversight”
- Help small business by creating a level playing field for providers
- Address and recognize that cloud risk is everywhere
- Improve cybersecurity outcomes with proactive management of security risks, strengths and threats

StateRAMP CJIS-Aligned Task Force


StateRAMP CJIS-Aligned Task Force
Local and State governments
StateRAMP Provider Members
Advisors from FBI CJIS Division
Advisors from StateRAMP

Also met with

- International Association of Chiefs of Police (IACP) Law Enforcement Information and Technology (LEIT) CJIS Working Group
- Integrated Justice Information Systems (IJIS) Institute

StateRAMP

StateRAMP CJIS Task Force

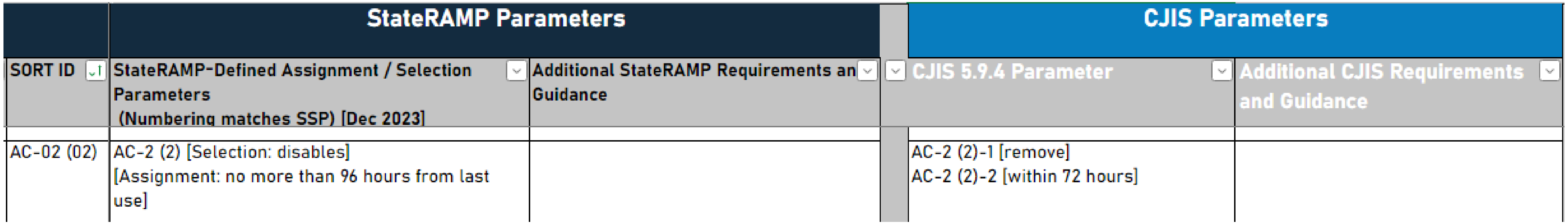
StateRAMP CJIS-Aligned Task Force

Our mission is to craft an innovative overlay for StateRAMP’s Moderate Impact Level baseline controls, aligning seamlessly with CJIS requirements. While a formal CJIS certification may not exist, our CJIS-focused overlay serves as a beacon, illuminating a product’s likelihood for CJIS conformance.

Scan the QR code to learn more about the task force.

StateRAMP CJIS-Aligned Overlay

- Examined StateRAMP Rev 5 Moderate impact level alignment with CJIS Security Policy 5.9.4
  - Compare the parameters of both frameworks where CJIS alignment with SP800-53
  - Some parameters StateRAMP is more restrictive; Others CJIS Policy is more restrictive
  - Create a CJIS overlay for StateRAMP where CJIS is more restrictive



	StateRAMP Parameters			CJIS Parameters	
SORT ID	StateRAMP-Defined Assignment / Selection Parameters (Numbering matches SSP) [Dec 2023]	Additional StateRAMP Requirements an Guidance		CJIS 5.9.4 Parameter	Additional CJIS Requirements and Guidance
AC-02 (02)	AC-2 (2) [Selection: disables] [Assignment: no more than 96 hours from last use]			AC-2 (2)-1 [remove] AC-2 (2)-2 [within 72 hours]	

> “Achieving a StateRAMP Authorization with the CJIS-aligned overlay will offer invaluable directional guidance, empowering agencies to make informed decisions about their cloud security solutions.”
>
> - Leah McGrath, Executive Director of StateRAMP.

Take the StateRAMP CJIS-Aligned Overlay Survey

The StateRAMP CJIS-Aligned Task Force is seeking feedback from CJIS professionals for our CJIS-Aligned overlay. The goal of this overlay is to simplify CJIS conformance for both the public and private sectors.

Scan the QR code and enter your email to receive the survey.

Cyber Summit 2024

StateRAMP Cyber Summit in Indianapolis, wit
h
presenting sponsor Carahsoft

- Wednesday, 9/11: State & Local CISO Symposium w/ Ctr. for Dig. Govt.
- Thursday, 9/12: Summit with Public & Private Sectors
- Friday, 9/13: Provider Leadership & 3PAO Advisory Councils

Complimentary for Public Sector to attend
Private Sector Registration

- *$500 *Special Member Registration
- $1,000 Member Registration
- $1,500 Non-Member Registration

Registration is open!
*Special Member Rates available through tiered memberships.

Scan the QR Code to register:

StateRAMP Cyber Summit 2024
presenting sponsor Carahsoft
Indianapolis, Indiana
***September 12, 2024**

Questions?

Take the StateRAMP CJIS-Aligned Overlay Survey

Scan the QR code and enter your
email to receive the survey.

PSTA

Public Safety Threat Alliance

Public Safety ISAO

Cyber Threats to Public Safety

“Building a network to protect public safety networks”

June 12, 2024

Jay Kaine
Director, PSTA

Tyler Brodbeck
Threat Intelligence Manager, PSTA

MOTOROLA SOLUTIONS

Public Safety Threat Alliance

Agenda

- Public Safety Threat Alliance
  - Mission & Information Sharing
- Public Safety Threat Landscape
  - Attack Trends
  - PSAP/CAD/LMR Threat Landscape
  - Mitigation Recommendations
- Q & A

PSTA

Public Safety Threat Alliance

Public Safety ISAO

PSTA Overview

MOTOROLA SOLUTIONS

PSTA
Public Safety Threat Alliance
Public Safety ISAO

Public Safety Threat Alliance

Focused Information and Intelligence Sharing

Our Mission

The Public Safety Threat Alliance, a **Cybersecurity and Infrastructure Security Agency (CISA)-recognized Information** Sharing and Analysis Organization, serves the global Public Safety community as a world-class information and threat intelligence sharing, collaboration and cybersecurity services hub, dedicated to improving Members' cybersecurity posture, defense, and resilience against ever-evolving threats to their no-fail Public Safety mission.

MOTOROLASOLUTIONS.COM/PSTA

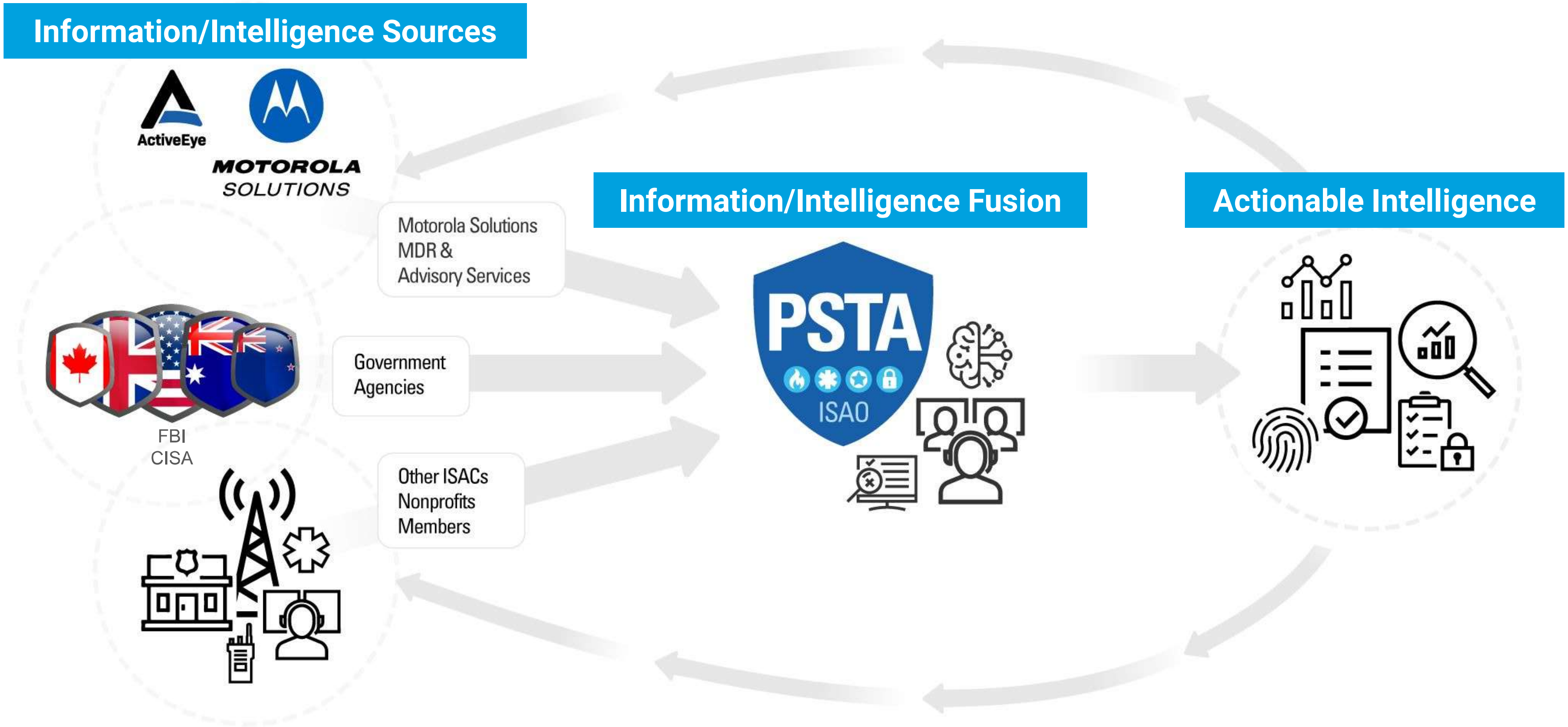
Concentrated
Threat intelligence and information sharing

Capable
Proactive defense solutions for public safety

Committed
Reduce the cybersecurity burden on agencies

Public Safety Threat Alliance

Information Sharing



Information/Intelligence Sources

Motorola Solutions MDR & Advisory Services

Government Agencies

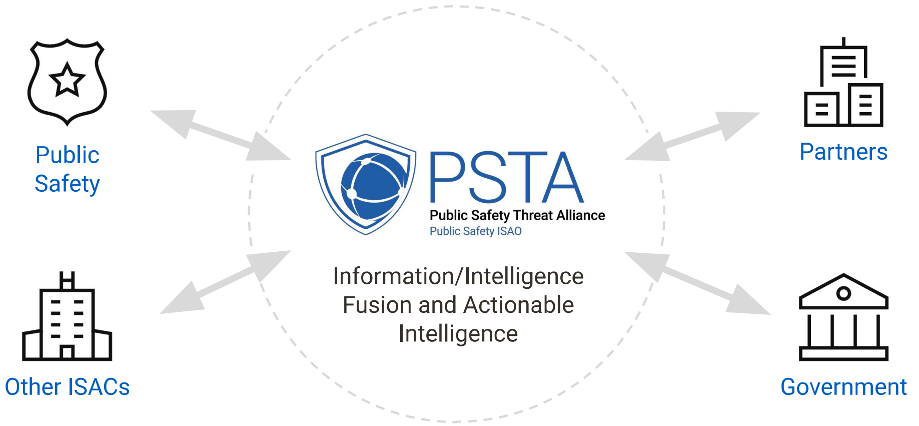
Other ISACs Nonprofits Members

Information/Intelligence Fusion

Actionable Intelligence

Public Safety Threat Alliance

USG Operational Collaboration


Public Safety
Partners
PSTA
Public Safety Threat Alliance
Public Safety ISAO
Information/Intelligence Fusion and Actionable Intelligence
Other ISACs
Government

JOINT CYBER DEFENSE COLLABORATIVE

SAFECOM NATIONWIDE SURVEY

FEMA

Public Safety Threat Alliance

Products & Services

COMPREHENSIVE ANALYSIS

Strategic & Tactical Analysis (Including TLP Amber/Red)

INTELLIGENCE PLATFORM

Mobile & Web Intelligence Platform Access (24/7)

ANALYST COLLABORATION

Analyst to Analyst Exchanges

DARKWEB INTEL

Darkweb Insights & Monitoring

ADVERSARY PLAYBOOKS

Adversary Tactical/Technical Playbooks

AUTOMATED THREAT FEED

Automated Threat Intelligence Feed

Public Safety Threat Alliance

Exercise KNIGHT SIREN

- Inaugural public safety wargaming effort
  - 4/29 in Grapevine, Texas
  - State/Provincial/Local participation from 10 states and 2 Canadian provinces
  - Federal government participation from CISA ECD and FBI Dallas Division Cyber Task Force
- Scenario-driven event
  - 8 event escalatory ransomware scenario (radio and 911 system impact)
  - Objectives:
    - Increase awareness of cyber threats and vulnerabilities
    - Strengthen incident response capabilities and coordination
    - Evaluate and enhance existing response plans and capabilities
    - Foster collaboration and relationships to improve preparedness
- Exercise lessons learned
  - Public safety emergency comms-focused CSIRP
  - Annual exercise of CSIRP
  - Containment strategies informed by data inventories
  - Build & exercise comms plan and external relationships before an attack

PSTA
Public Safety Threat Alliance
Public Safety ISAO

Public Safety Threat Landscape

MOTOROLA SOLUTIONS

Threat impact on public safety

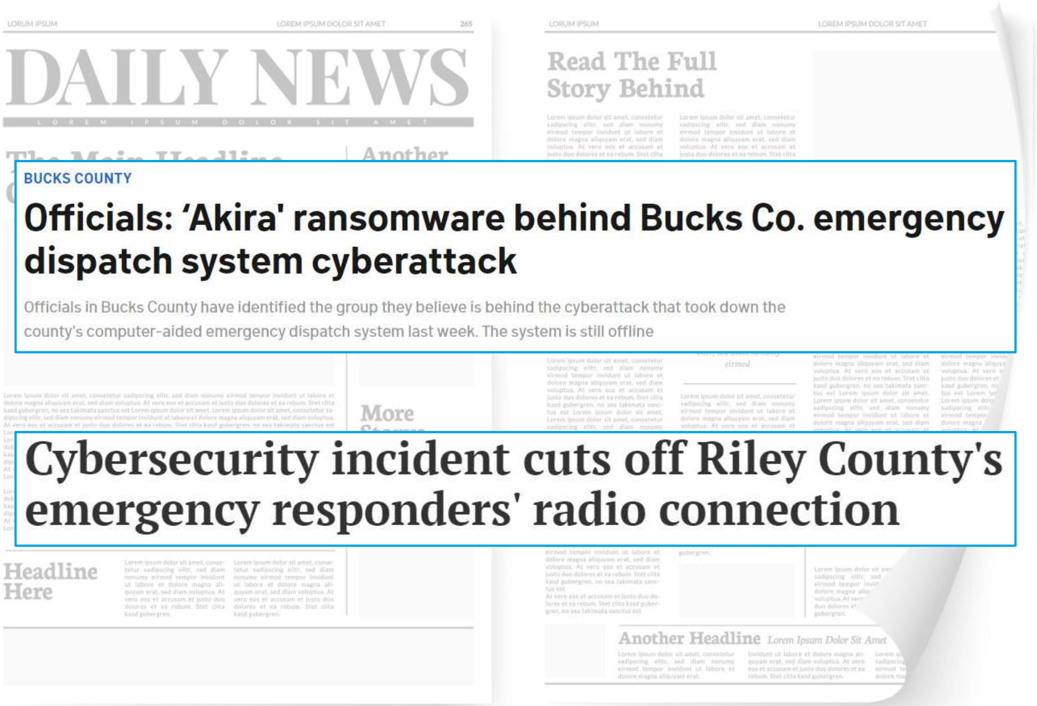
ACTUAL INCIDENTS (2024)

Pennsylvania:

- CAD system “Crippled” for 9 days
- 9-1-1 call handling remained operational through backup procedures
- Dispatch radio communications “kept to essential transmissions only”
- Cost at least $572k USD just for remediation

Kansas:

- Threat Actor gained access via exposed and insecure VPN with direct access to LMR Network
- Hackers shut down primary public safety P25 network impacting all local police, fire, and emergency services
- Forced to migrate to the statewide Dept. of Transportation radio network



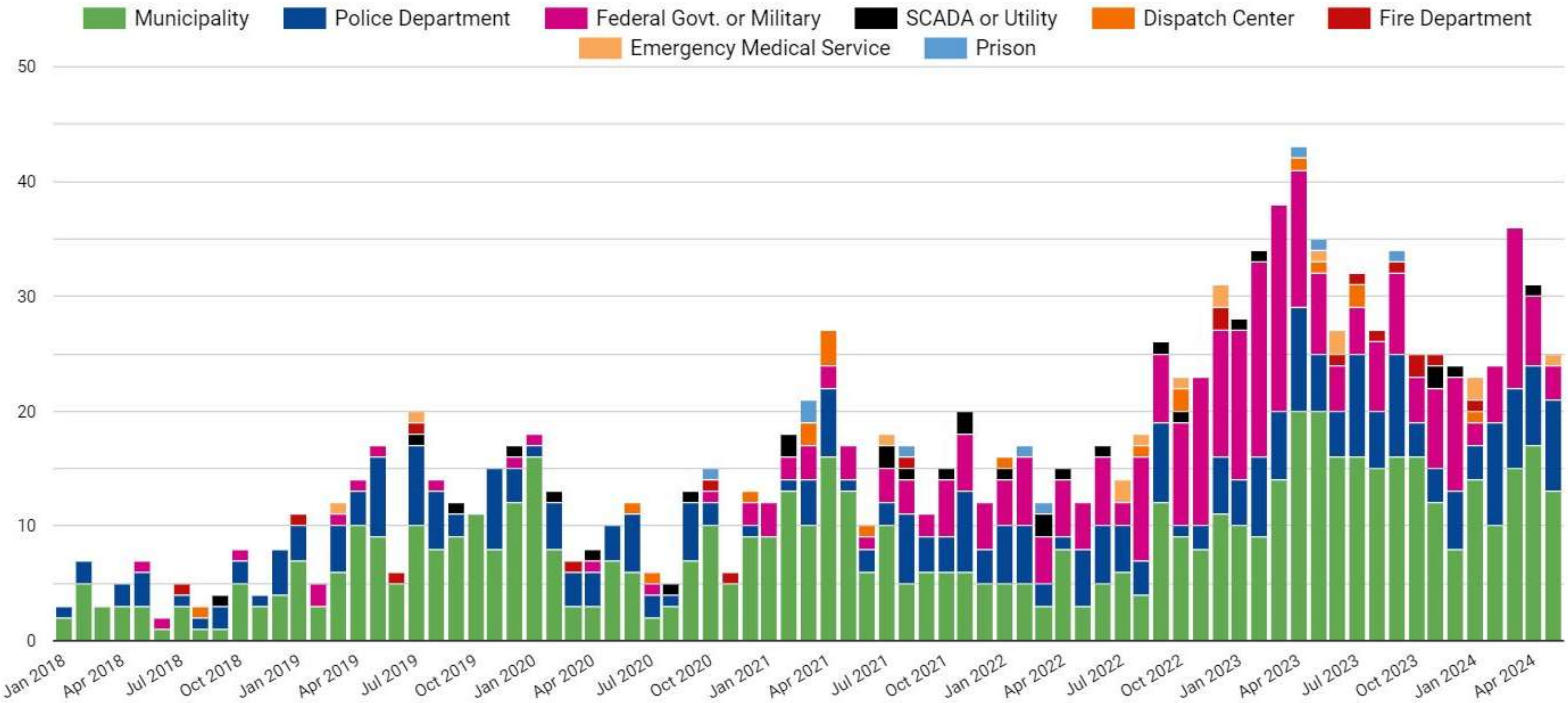
BUCKS COUNTY

Officials: ‘Akira' ransomware behind Bucks Co. emergency dispatch system cyberattack

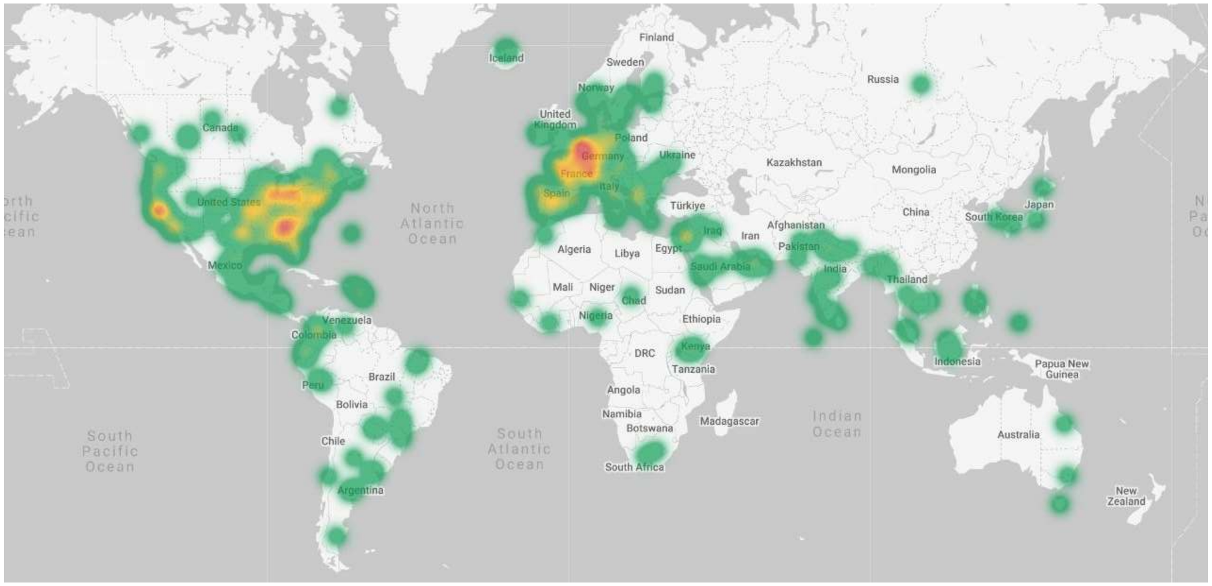
Officials in Bucks County have identified the group they believe is behind the cyberattack that took down the county's computer-aided emergency dispatch system last week. The system is still offline

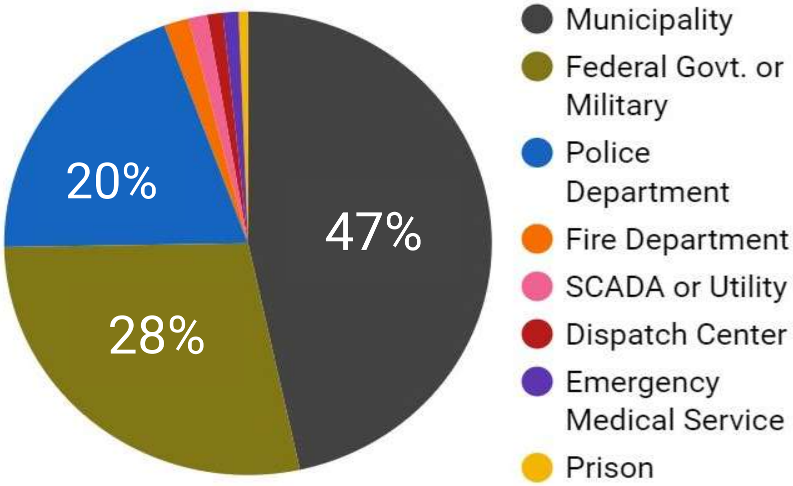
Cybersecurity incident cuts off Riley County's emergency responders' radio connection

Successful cyberattacks to Public Safety

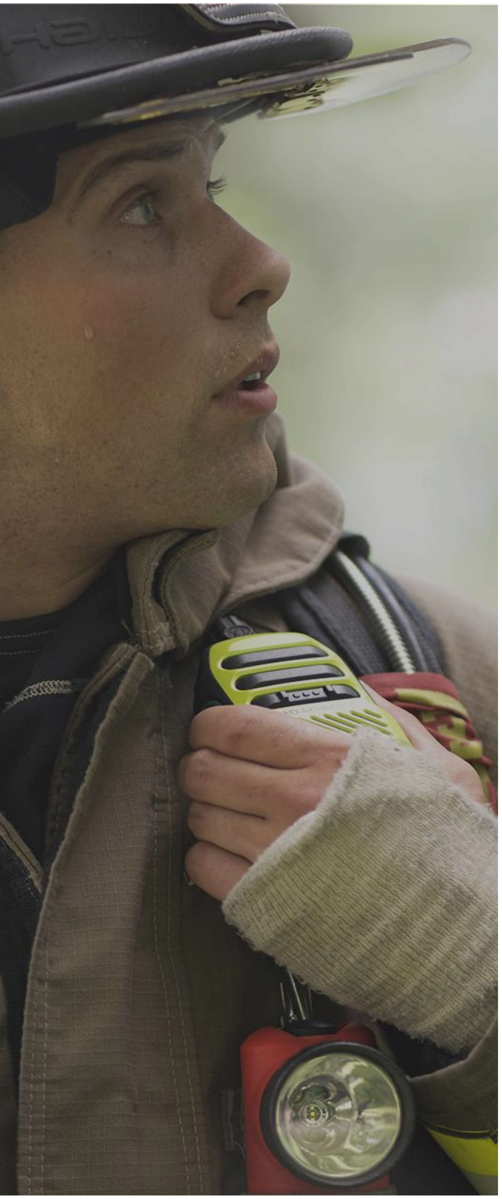


Where hackers prefer to operate



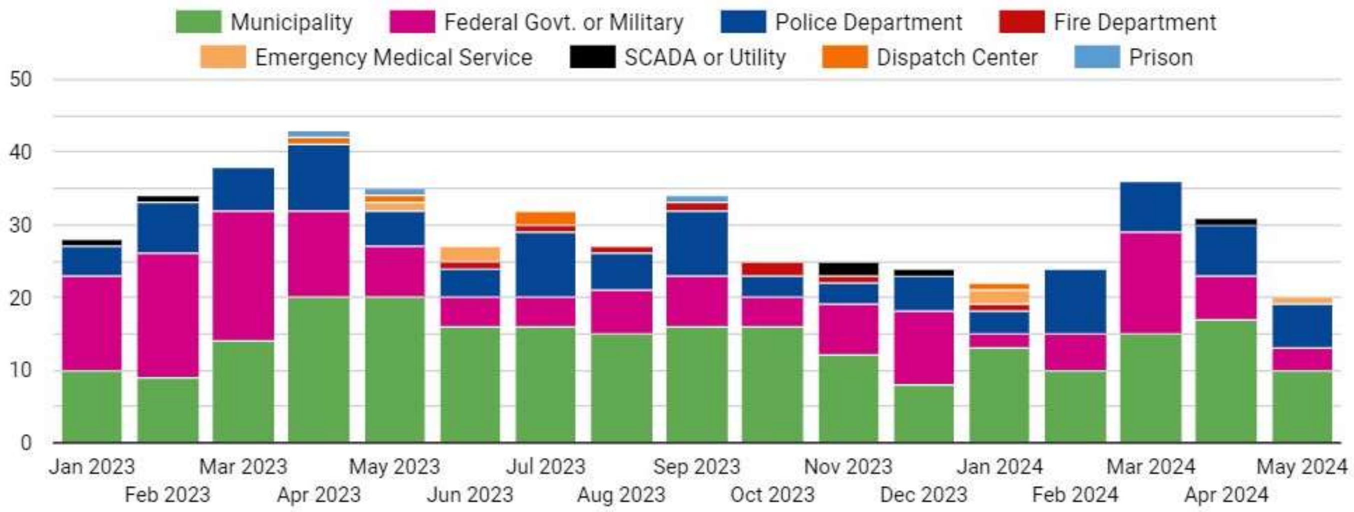


01 January 2023 - 29 May 2024



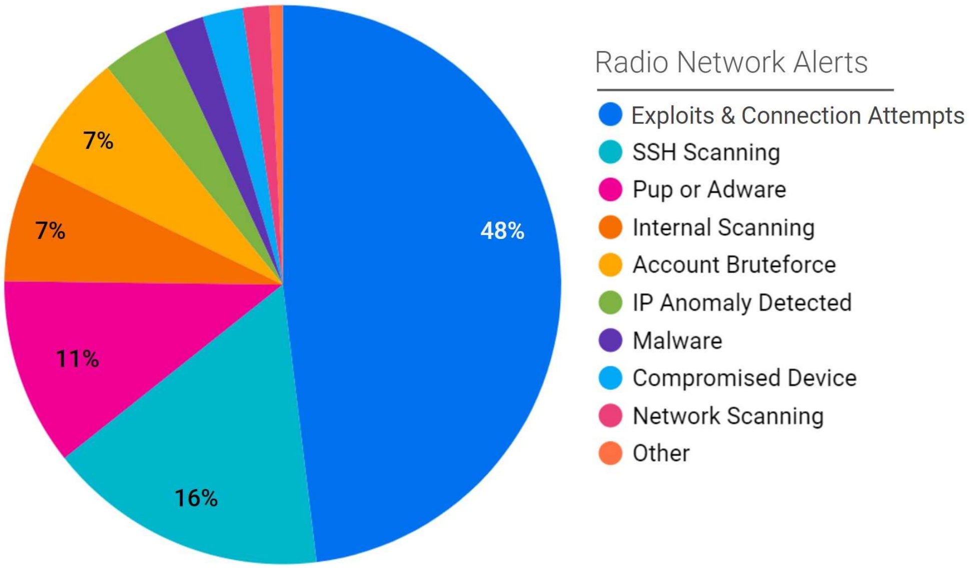
2024 PSTA observations

- **11** cyberattacks shut down critical emergency services systems
- Cyberattacks on law enforcement in Q1 ‘24 grew **64%** over Q4 ‘23
- One cyber attack compromised a public safety agency every day



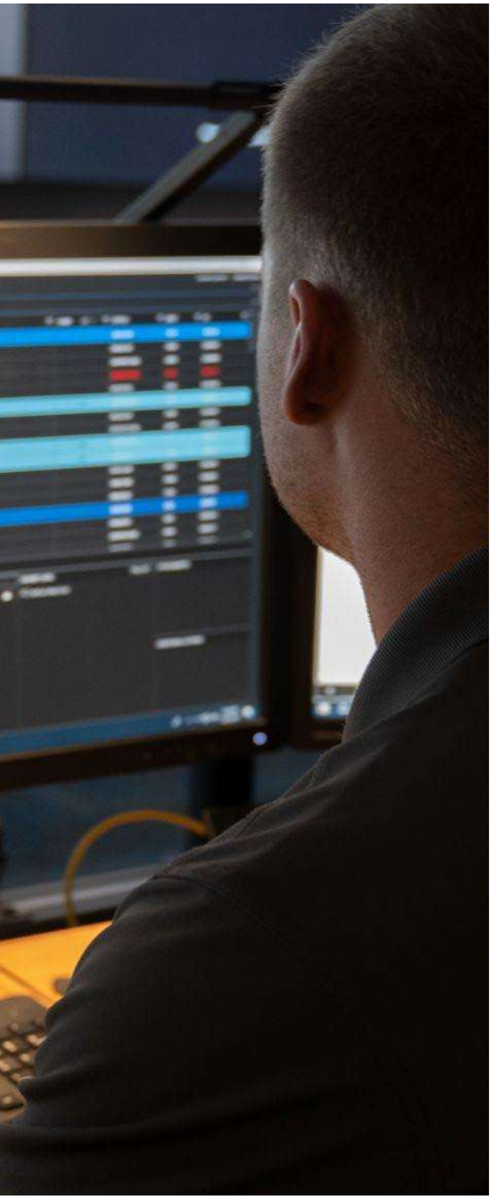
Cyber disruptions to land mobile radio

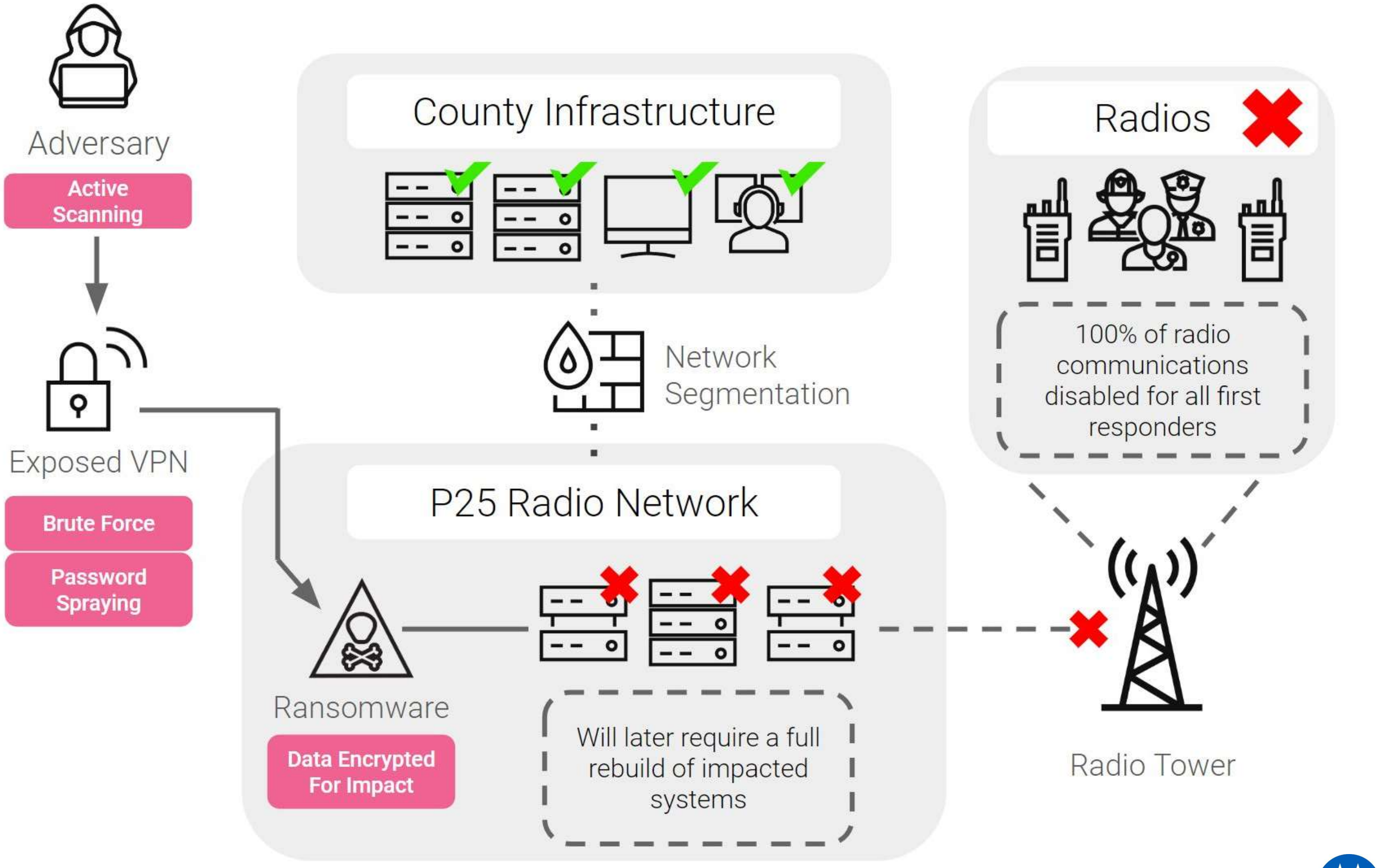
- **4** cyberattacks have degraded LMR operations since 2023
  - **3** in 2024
- **All** attacks involved ransomware
  - Average downtime was **7** days; **2** day minimum
- **All** victims were located in the U.S.



Top radio network activity mitigated by ActiveEye since January 2023

2024 LMR Attack





Adversary

Active Scanning

Exposed VPN

Brute Force

Password Spraying

County Infrastructure

Network Segmentation

P25 Radio Network

Ransomware

Data Encrypted For Impact

Will later require a full rebuild of impacted systems

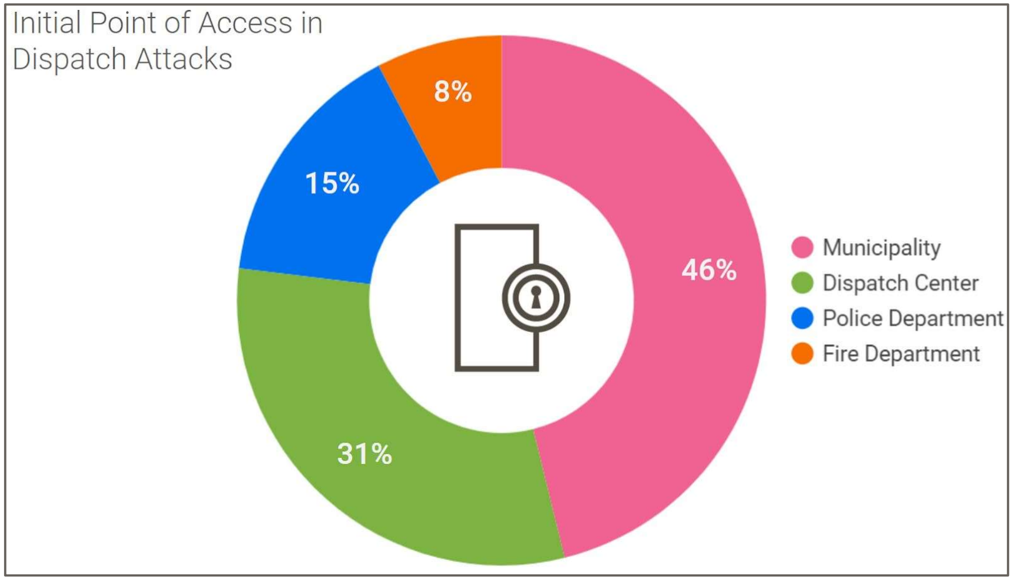
Radios

100% of radio communications disabled for all first responders

Radio Tower

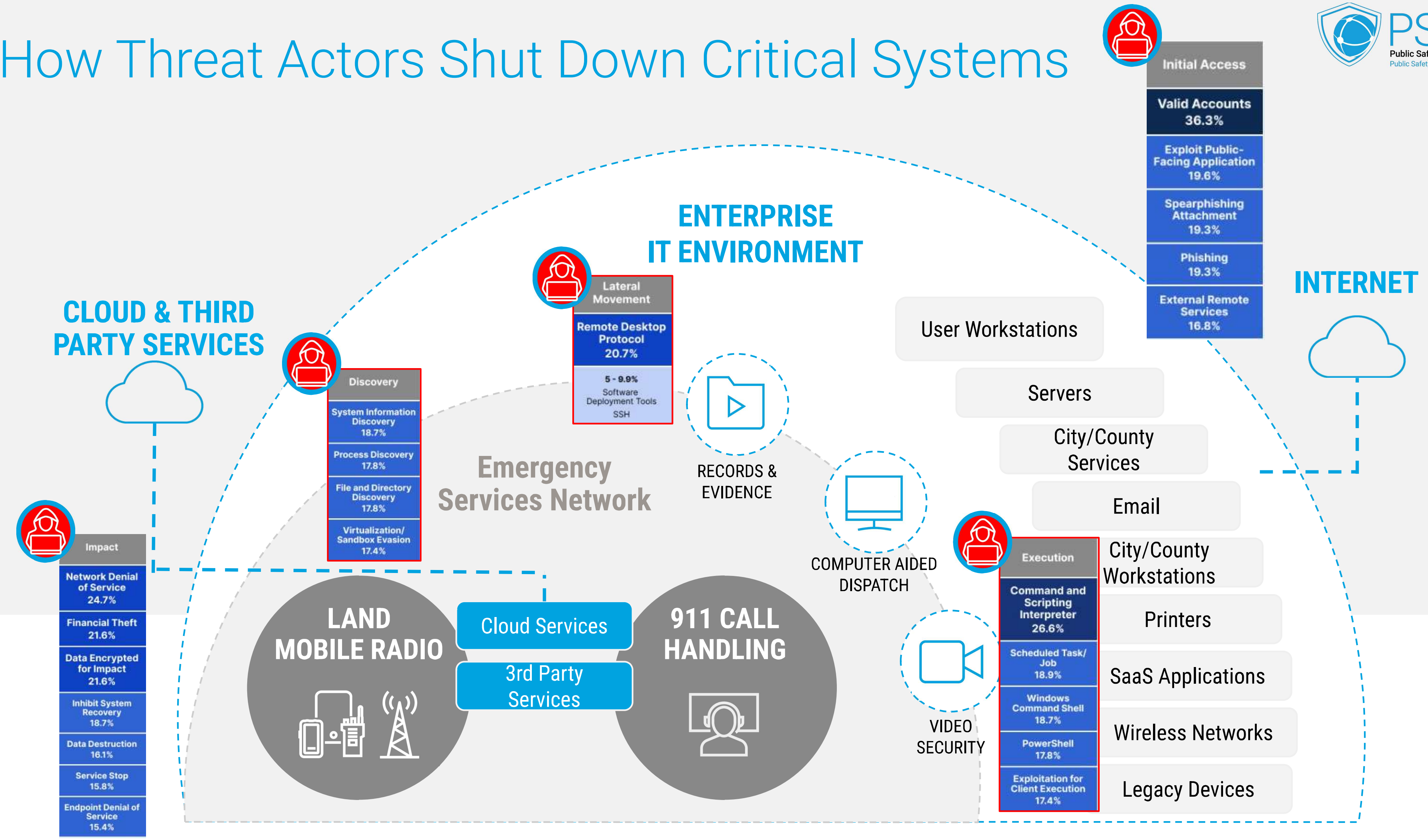
Cyber Disruptions to 9-1-1/ Dispatch Centers

- **19** cyberattacks have degraded CAD operations since 2023
  - **12** total cyberattacks degraded CAD operations 2019-2022
- **90%** of observed 2023 attacks involved ransomware
  - Average downtime was **15** days; **5** day minimum
- **77%** of CAD and PSAP victims were located in the U.S.



How Threat Actors Shut Down Critical Systems

PSTA
Public Safety Threat Alliance
Public Safety ISAO



Initial Access
Valid Accounts 36.3%
Exploit Public-Facing Application 19.6%
Spearphishing Attachment 19.3%
Phishing 19.3%
External Remote Services 16.8%

Lateral Movement
Remote Desktop Protocol 20.7%
5 - 9.9% Software Deployment Tools SSH

Discovery
System Information Discovery 18.7%
Process Discovery 17.8%
File and Directory Discovery 17.8%
Virtualization/ Sandbox Evasion 17.4%

Execution
Command and Scripting Interpreter 26.6%
Scheduled Task/ Job 18.9%
Windows Command Shell 18.7%
PowerShell 17.8%
Exploitation for Client Execution 17.4%

Impact
Network Denial of Service 24.7%
Financial Theft 21.6%
Data Encrypted for Impact 21.6%
Inhibit System Recovery 18.7%
Data Destruction 16.1%
Service Stop 15.8%
Endpoint Denial of Service 15.4%

Reconnaissance

- Phishing for Information 13.7%
- 0.1 - 4.9 %
  - Credentials
  - Active Scanning

Resource Development

- Tool 16.2%
- Malware 14.3%
- 5 - 9.9%
  - Domains
  - Acquire Access
- 0.1 - 4.9 %
  - Malvertising
  - Virtual Private Server
  - SEO Poisoning
  - Compromise Accounts
  - Develop Capabilities
  - Exploits

Initial Access

- Valid Accounts 36.3%
- Exploit Public-Facing Application 19.6%
- Spearphishing Attachment 19.3%
- Phishing 19.3%
- External Remote Services 16.8%
- Spearphishing Link 12.2%
- Supply Chain Compromise 11.9%
- 5 - 9.9%
  - Local Accounts
  - Drive-by Compromise
- 0.1 - 4.9 %
  - Domain Accounts
  - Compromise Software Supply Chain
  - Spearphishing via Service
  - Drive-by Compromise

Execution

- Command and Scripting Interpreter 26.6%
- Scheduled Task/ Job 18.9%
- Windows Command Shell 18.7%
- PowerShell 17.8%
- Exploitation for Client Execution 17.4%
- Service Execution 13.7%
- Windows Management Instrumentation 12.8%
- Malicious File 10.2%
- 5 - 9.9%
  - User Execution
  - Visual Basic
  - Software Deployment Tools
  - Python
  - Native API
- 0.1 - 4.9 %
  - System Services

Persistence

- Valid Accounts 23%
- Scheduled Task/ Job 18.9%
- External Remote Services 16.8%
- Account Manipulation 10.5%
- Create Account 10.5%
- 5 - 9.9%
  - Windows Service
  - Local Accounts
  - DLL Side-Loading
  - Boot or Logon Autostart Execution
- 0.1 - 4.9 %
  - Domain Accounts
  - Local Account

Privilege Escalation

- Valid Accounts 23.6%
- Scheduled Task/ Job 18.9%
- Exploitation for Privilege Escalation 14.3%
- Process Injection 14%
- Group Policy Modification 13%
- Account Manipulation 10.5%
- Bypass User Account Control 10.5%
- 5 - 9.9%
  - Windows Service
  - Local Accounts
  - DLL Side-Loading
  - Boot or Logon Autostart Execution
- 0.1 - 4.9 %
  - Domain Accounts
  - Dynamic-link Library Injection
  - Access Token Manipulation
  - Abuse Elevation Control Mechanism
  - Portable Executable Injection
  - Create Process with Token

Defense Evasion

- Obfuscated Files or Information 27.7%
- Valid Accounts 23.6%
- Disable or Modify Tools 19.3%
- Virtualization/ Sandbox Evasion 17.4%
- Modify Registry 15.5%
- Deobfuscate/ Decode Files or Information 14.3%
- Process Injection 14%
- Clear Windows Event Logs 12.8%
- Disable or Modify System Firewall 12.2%
- Match Legitimate Name or Location 11.9%
- Bypass User Account Control 11.4%
- Software Packing 10.8%
- Indicator Removal 10.8%

Credential Access

- Brute Force 17.9%
- OS Credential Dumping 12%
- LSASS Memory 12%
- 5 - 9.9%
  - Keylogging
- 0.1 - 4.9 %
  - Adversary-in-the-Middle
  - Credential Stuffing
  - Kerberoasting
  - Exploitation for Credential Access
  - NTDS
  - Steal or Forge Authentication Certificates
  - Network Sniffing
  - Multi-Factor Authentication Request Generation
  - Group Policy Preferences
  - LSA Secrets
  - Password Spraying
  - Password Guessing
  - Password Cracking
  - Unsecured Credentials
  - Credentials In Files

Discovery

- System Information Discovery 18.7%
- Process Discovery 17.8%
- File and Directory Discovery 17.8%
- Virtualization/ Sandbox Evasion 17.4%
- Remote System Discovery 12.8%
- System Service Discovery 10.5%
- 5 - 9.9%
  - Debugger Evasion
  - Network Service Discovery
  - Network Share Discovery
  - System Language Discovery
  - Peripheral Device Discovery
- 0.1 - 4.9 %
  - System Network Connections Discovery
  - Query Registry
  - Domain Account
  - System Owner/User Discovery
  - Network Sniffing
  - System Time Discovery
  - System Network Configuration Discovery
  - Domain Trust Discovery

Lateral Movement

- Remote Desktop Protocol 20.7%
- 5 - 9.9%
  - Software Deployment Tools
  - SSH
- 0.1 - 4.9 %
  - Lateral Tool Transfer
  - RDP Hijacking

Collection

- Data from Local System 19%
- Screen Capture 12.8%
- 5 - 9.9%
  - Keylogging
- 0.1 - 4.9 %
  - Adversary-in-the-Middle

Command and Control

- Remote Access Software 18.9%
- Web Protocols 16.9%
- Ingress Tool Transfer 16.6%
- Multi-hop Proxy 12.2%
- 5 - 9.9%
  - Protocol Tunneling
  - Domain Fronting
- 0.1 - 4.9 %
  - Non-Application Layer Protocol
  - Encrypted Channel
  - Web Service
  - File Transfer Protocols

Impact

- Network Denial of Service 24.7%
- Financial Theft 21.6%
- Data Encrypted for Impact 21.6%
- Inhibit System Recovery 18.7%
- Data Destruction 16.1%
- Service Stop 15.8%
- Endpoint Denial of Service 15.4%
- 5 - 9.9%
  - Resource Hijacking
- 0.1 - 4.9 %
  - Direct Network Flood
  - Account Access Removal
  - Defacement
  - System Shutdown/ Reboot

Defense Evasion 5 - 9.9%

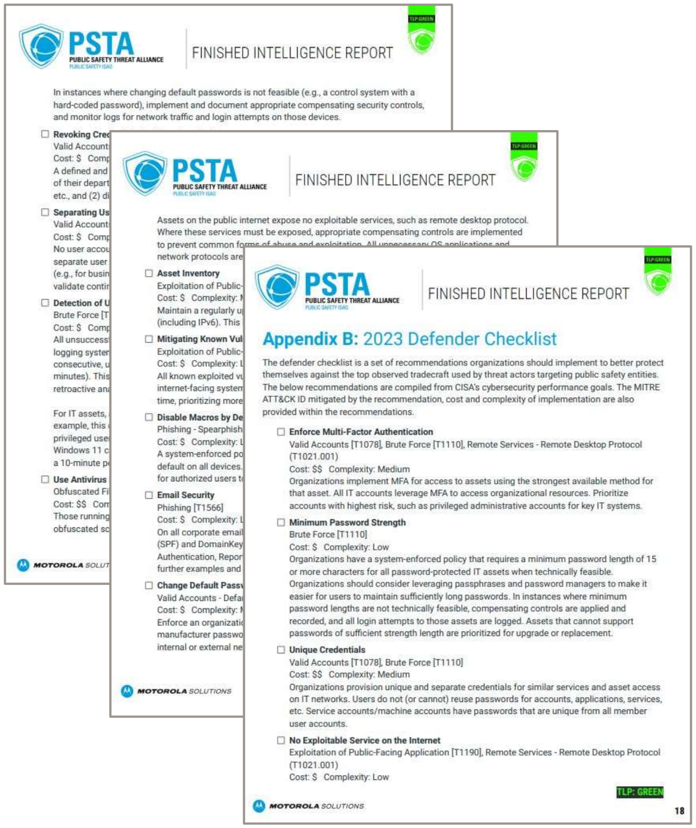
- Debugger Evasion
- Code Signing
- File Deletion
- Local Accounts
- Safe Mode Boot
- Mark-of-the-Web Bypass
- Environmental Keying
- Domain Policy Modification
- Mshta

Defense Evasion 0.1 - 4.9 %

- Masquerading
- Timestomp
- Command Obfuscation
- Domain Accounts
- HTML Smuggling
- Windows File and Directory Permissions Modification
- Impersonation
- Impair Defenses
- Dynamic-link Library Injection
- Create Cloud Instance
- Access Token Manipulation
- Abuse Elevation Control Mechanism
- Rootkit
- Reflective Code Loading
- Portable Executable Injection
- Hidden Window
- Create Process with Token

How to Use This Intelligence

PSTA
Public Safety Threat Alliance
Public Safety ISAO



PSTA PUBLIC SAFETY THREAT ALLIANCE PUBLIC SAFETY ISAO | FINISHED INTELLIGENCE REPORT

TLP:GREEN

In instances where changing default passwords is not feasible (e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices.

□ **Revoking Cre**
Valid Account
Cost: $ Comp
A defined and
of their depart
etc., and (2) di

□ **Separating Us**
Valid Account
Cost: $ Comp
No user accou
separate user
(e.g., for busin
validate contir

□ **Detection of U**
Brute Force [T
Cost: $ Comp
All unsuccess
logging syster
consecutive, u
minutes). This
retroactive ana

For IT assets,
example, this
privileged use
Windows 11 c
a 10-minute pe

□ **Use Antivirus**
Obfuscated Fi
Cost: $$ Com
Those running
obfuscated sc

MOTOROLA SOLUT

PSTA PUBLIC SAFETY THREAT ALLIANCE PUBLIC SAFETY ISAO | FINISHED INTELLIGENCE REPORT

TLP:GREEN

Assets on the public internet expose no exploitable services, such as remote desktop protocol.
Where these services must be exposed, appropriate compensating controls are implemented
to prevent common fo
network protocols are

□ **Asset Inventory**
Exploitation of Public-
Cost: $ Complexity: M
Maintain a regularly u
(including IPv6). This

□ **Mitigating Known Vul**
Exploitation of Public-
Cost: $ Complexity: L
All known exploited vu
internet-facing system
time, prioritizing more

□ **Disable Macros by De**
Phishing - Spearphish
Cost: $ Complexity: L
A system-enforced po
default on all devices.
for authorized users t

□ **Email Security**
Phishing [T1566]
Cost: $ Complexity: L
On all corporate email
(SPF) and DomainKey
Authentication, Repor
further examples and

□ **Change Default Passw**
Valid Accounts - Defa
Cost: $ Complexity: M
Enforce an organizatio
manufacturer passwo
internal or external ne

MOTOROLA SOLUTIONS

PSTA PUBLIC SAFETY THREAT ALLIANCE PUBLIC SAFETY ISAO | FINISHED INTELLIGENCE REPORT

TLP:GREEN

Appendix B: 2023 Defender Checklist

The defender checklist is a set of recommendations organizations should implement to better protect themselves against the top observed tradecraft used by threat actors targeting public safety entities. The below recommendations are compiled from CISA's cybersecurity performance goals. The MITRE ATT&CK ID mitigated by the recommendation, cost and complexity of implementation are also provided within the recommendations.

□ **Enforce Multi-Factor Authentication**
Valid Accounts [T1078], Brute Force [T1110], Remote Services - Remote Desktop Protocol (T1021.001)
Cost: $$ Complexity: Medium
Organizations implement MFA for access to assets using the strongest available method for that asset. All IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems.

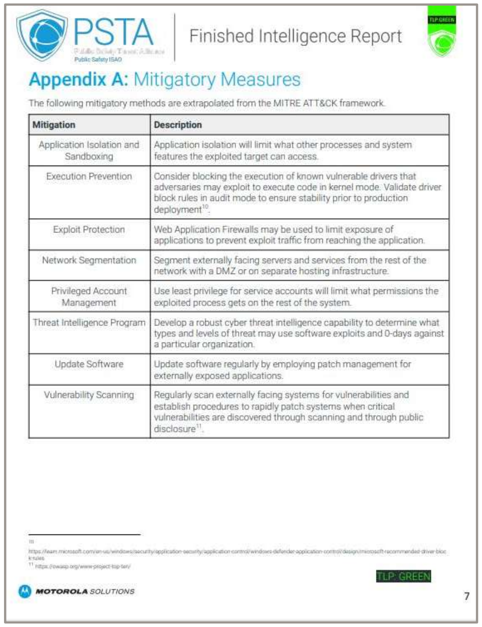
□ **Minimum Password Strength**
Brute Force [T1110]
Cost: $ Complexity: Low
Organizations have a system-enforced policy that requires a minimum password length of 15 or more characters for all password-protected IT assets when technically feasible. Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement.

□ **Unique Credentials**
Valid Accounts [T1078], Brute Force [T1110]
Cost: $$ Complexity: Medium
Organizations provision unique and separate credentials for similar services and asset access on IT networks. Users do not (or cannot) reuse passwords for accounts, applications, services, etc. Service accounts/machine accounts have passwords that are unique from all member user accounts.

□ **No Exploitable Service on the Internet**
Exploitation of Public-Facing Application [T1190], Remote Services - Remote Desktop Protocol (T1021.001)
Cost: $ Complexity: Low

TLP: GREEN

MOTOROLA SOLUTIONS 18



PSTA Public Safety Threat Alliance Public Safety ISAO | Finished Intelligence Report

TLP:GREEN

Appendix A: Mitigatory Measures

The following mitigatory methods are extrapolated from the MITRE ATT&CK framework.

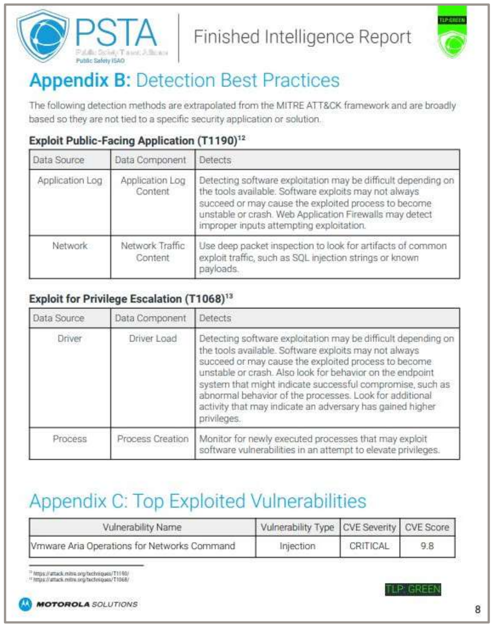
Mitigation	Description
Application Isolation and Sandboxing	Application isolation will limit what other processes and system features the exploited target can access.
Execution Prevention	Consider blocking the execution of known vulnerable drivers that adversaries may exploit to execute code in kernel mode. Validate driver block rules in audit mode to ensure stability prior to production deployment[10].
Exploit Protection	Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application.
Network Segmentation	Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.
Privileged Account Management	Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system.
Threat Intelligence Program	Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization.
Update Software	Update software regularly by employing patch management for externally exposed applications.
Vulnerability Scanning	Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure[11].

[10] https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/microsoft-recommended-driver-block-rules

[11] https://owasp.org/www-project-top-ten/

TLP: GREEN

MOTOROLA SOLUTIONS 7



PSTA Public Safety Threat Alliance Public Safety ISAO | Finished Intelligence Report

TLP:GREEN

Appendix B: Detection Best Practices

The following detection methods are extrapolated from the MITRE ATT&CK framework and are broadly based so they are not tied to a specific security application or solution.

Exploit Public-Facing Application (T1190)[12]

Data Source	Data Component	Detects
Application Log	Application Log Content	Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash. Web Application Firewalls may detect improper inputs attempting exploitation.
Network	Network Traffic Content	Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection strings or known payloads.

Exploit for Privilege Escalation (T1068)[13]

Data Source	Data Component	Detects
Driver	Driver Load	Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash. Also look for behavior on the endpoint system that might indicate successful compromise, such as abnormal behavior of the processes. Look for additional activity that may indicate an adversary has gained higher privileges.
Process	Process Creation	Monitor for newly executed processes that may exploit software vulnerabilities in an attempt to elevate privileges.

Appendix C: Top Exploited Vulnerabilities

Vulnerability Name	Vulnerability Type	CVE Severity	CVE Score
Vmware Aria Operations for Networks Command	Injection	CRITICAL	9.8

[12] https://attack.mitre.org/techniques/T1190/

[13] https://attack.mitre.org/techniques/T1068/

TLP: GREEN

MOTOROLA SOLUTIONS 8

PSTA
Public Safety Threat Alliance
Public Safety ISAO

Mitigation recommendations

- Establish **offline** back-ups and become practiced in restoring affected systems
- Prioritize **patching internet-facing systems**, focusing on flaws which could allow for remote-code-execution
- **Enforce MFA**, prioritizing internet-facing systems
- **Be aware** of connections to municipal networks
- Adopt **24/7 monitoring**
- **Join** information/intelligence sharing organizations (ISAOs/ISACs)

PSTA

Public Safety Threat Alliance

Public Safety ISAO

Q & A

MOTOROLA SOLUTIONS

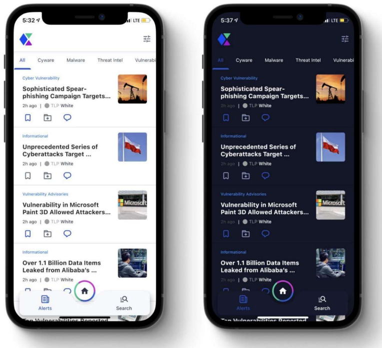
PSTA
Public Safety Threat Alliance
Public Safety ISAO

Public Safety Threat Alliance

Membership

Membership Tier	Fee	Info Sharing Agreement	Webinars	TLP Clear/Green Products	TLP Amber/Red Products	Analyst Call Participation	Secure Platform Access *	Dark Web Monitoring	Automated Feed (2024)
Associate	No Cost		X	X					
Full Access	No Cost	X	X	X	X	X	X	X	X
Strategic Partner	No Cost	X	X	X	X	X	X	X	X

** Secure Platform Access: (PS Dashboard, Daily Feed, Secure Chat with PSTA Analysts, Mobile App, Etc.)*



Cyber Vulnerability
Sophisticated Spear-phishing Campaign Targets...
2h ago | TLP White

Informational
Unprecedented Series of Cyberattacks Target ...
2h ago | TLP White

Vulnerability Advisories
Vulnerability in Microsoft Paint 3D Allowed Attackers...
2h ago | TLP White

Informational
Over 1.1 Billion Data Items Leaked from Alibaba's ...
2h ago | TLP White

Associate: public sector and non-profit organizations (email distribution only)

Full Access: public sector and non-profit organizations with a signed PSTA information sharing agreement in place

Strategic Partner: private companies with a signed PSTA information sharing agreement in place (launch date: 4Q23)

*Each organization is strongly encouraged to have at least one representative with secure portal access, to obtain the **most up-to-date and actionable intelligence** from the PSTA and its partners!*

PSTA
Public Safety Threat Alliance
Public Safety ISAO

Public Safety Threat Alliance

“Building a network to protect public safety networks

Continued Momentum

- Public service established in 2022
- 1,200+ public safety member organizations
- 85% members are North America based, remainder in LATAM, EU and ANZ

Operational Impact

- Regular production/sharing of public safety-focused intelligence at no-cost
- Consistent positive feedback from PSTA member base
- Automated indicator feed live

Member Org CISO (Texas)

“Membership in the PSTA has proven to be immensely helpful for our organization. The specialized alerts, insightful intelligence products, and coordination for public safety are truly unparalleled.”

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Considerations for Implementing MFA to Protect Criminal Justice Information

NIST Information Technology Lab

Applied Cybersecurity Division

National Cybersecurity Center of Excellence

This webinar is being recorded

June 13th, 2024

Agenda

- Opening Remarks
- Introductions
- Project Overview
- MFA deployment Considerations
- MFA Use Cases
- Discussion & Questions

Opening Remarks

Team Introduction

Bill Fisher
Security Engineer,
NCCoE

Sudhi Umarji
ICAM Engineer, MITRE
Coporation

DISCLAIMER

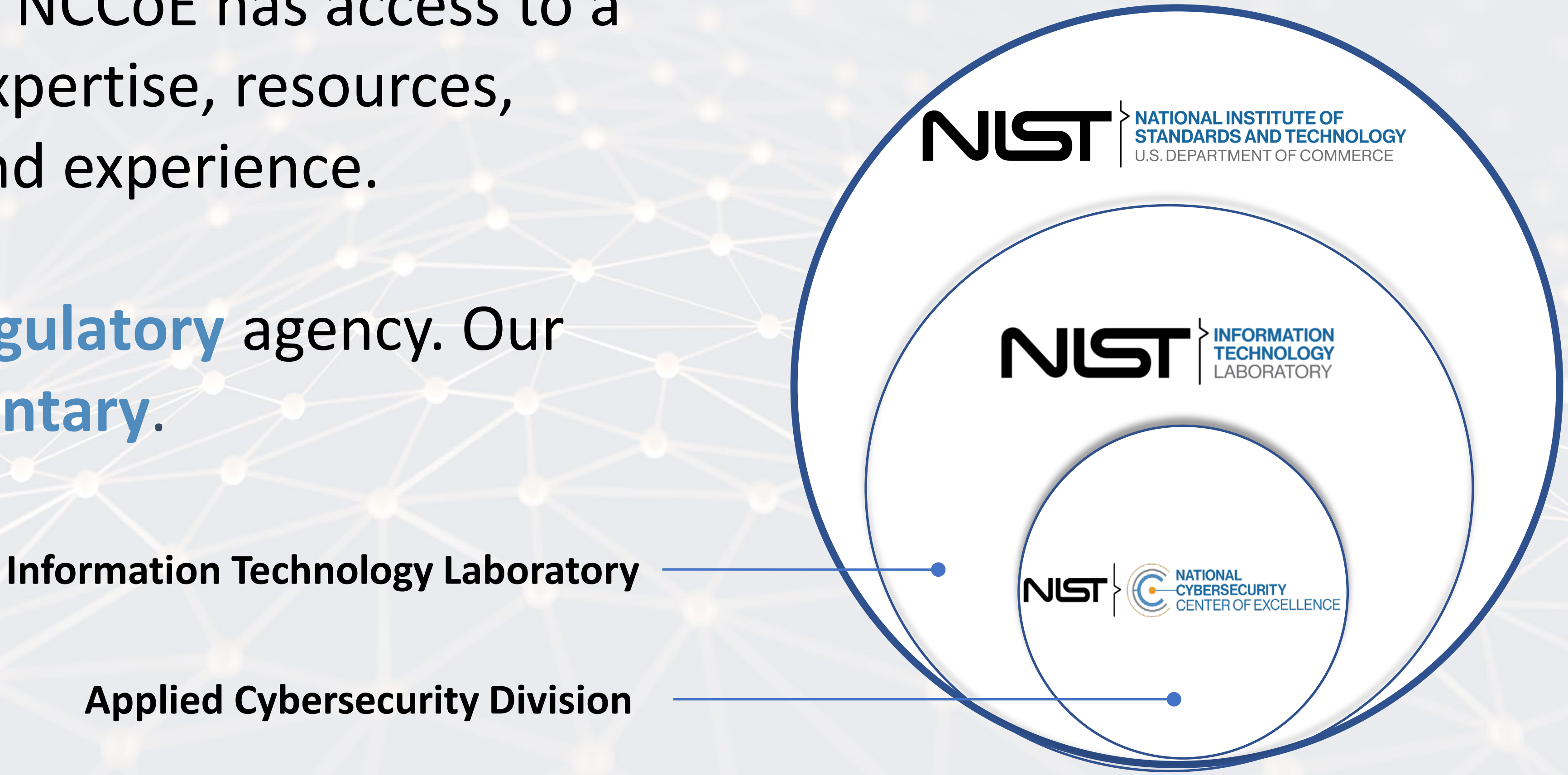
The information in this presentation is intended to aid agencies in their MFA implementations but in no way guarantees that their implementation will meet CJIS Security Policy requirements or will pass a CJIS audit.

All questions for how a specific MFA implementation can meet the CJIS Security Policy should be directed to the CJIS ISO team at iso@fbi.gov.

Who is the NCCoE

Part of NIST, the NCCoE has access to a foundation of expertise, resources, relationships, and experience.

NIST is a **non-regulatory** agency. Our guidance is **voluntary**.


NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE
NIST INFORMATION TECHNOLOGY LABORATORY
NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
Information Technology Laboratory
Applied Cybersecurity Division

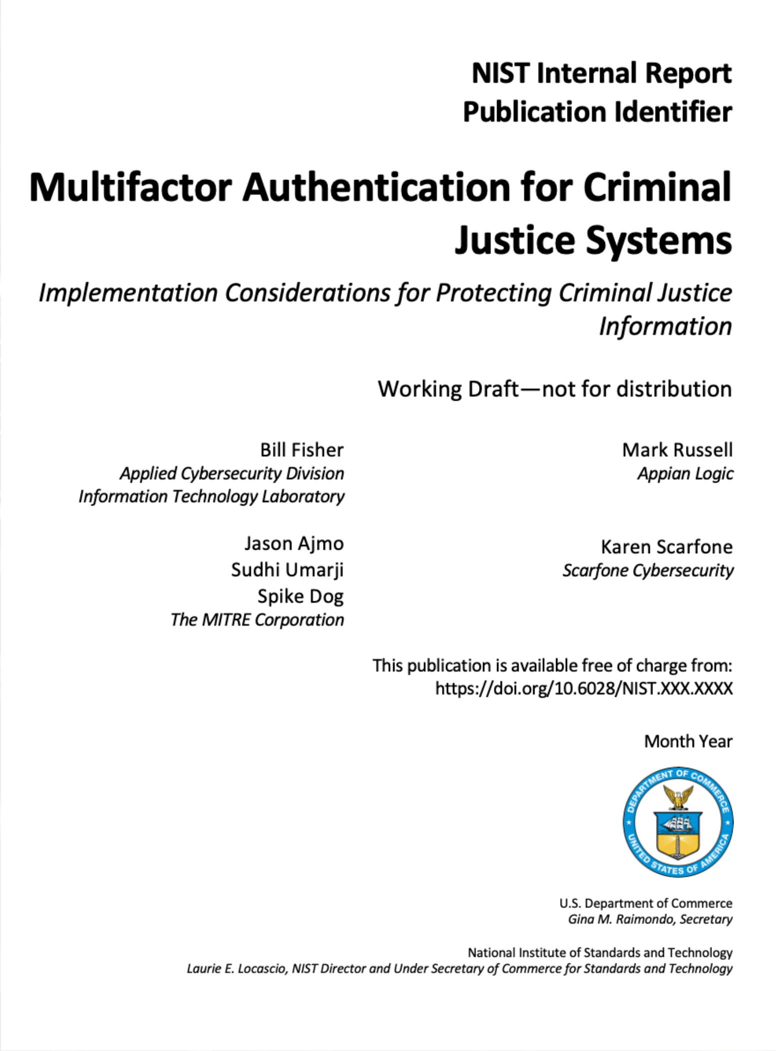
NCCoE MFA Project Overview

Background: 8+ years of working with Public Safety communities and their cybersecurity challenges.

Project Goal: Assist agencies nationwide who need access to CJI with their MFA implementations.

Methodology: We’ve spent the last 6 months chatting with agencies around the county about MFA use cases, technologies and pain points.

Output: A NISTIR detailing what we learned and considerations for implementing MFA in the context of criminal justice systems.



NIST Internal Report
Publication Identifier

Multifactor Authentication for Criminal Justice Systems

Implementation Considerations for Protecting Criminal Justice Information

Working Draft—not for distribution

Bill Fisher
Applied Cybersecurity Division
Information Technology Laboratory

Mark Russell
Appian Logic

Jason Ajmo
Sudhi Umarji
Spike Dog
The MITRE Corporation

Karen Scarfone
Scarfone Cybersecurity

This publication is available free of charge from:
https://doi.org/10.6028/NIST.XXX.XXXX

Month Year

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

During this workshop…

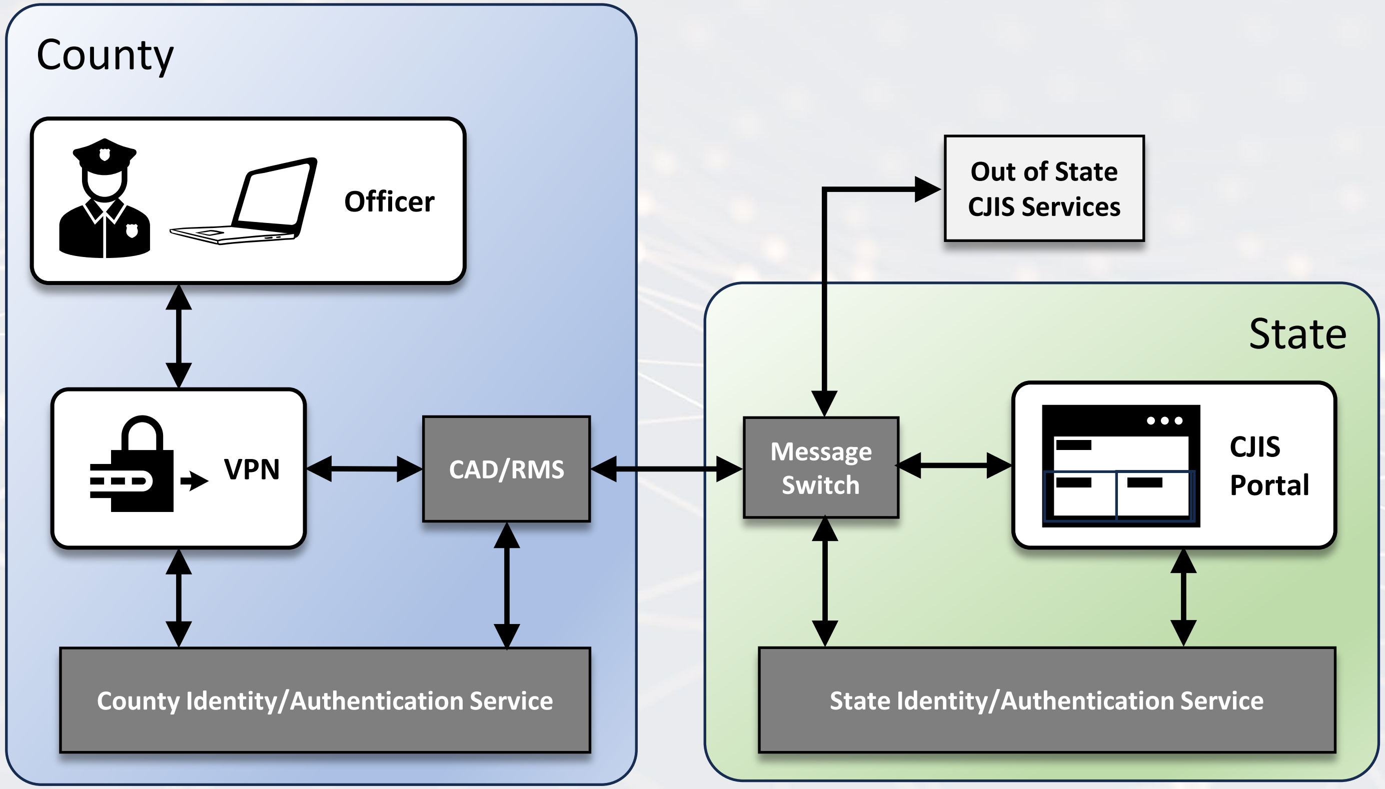
We hope to foster a greater understanding of the technology, architectures, challenges and potential MFA options for protecting CJI. Two common themes:

"It Depends" – there are many ways to implement MFA. What works for one organization or user base may not be best for another. This webinar seeks to explore many different architectures and to provide some key MFA implementation principles should be consider across all implementations.

"It Takes a Village" – CJI systems are used across state, local, tribal and territorial governments with both criminal and non-criminal justice agencies. Accessing CJI often requires the cross-jurisdictional connection of information technology systems and collaboration between multiple agencies. Everyone on this call has a role to play in helping agencies implement MFA.

What we have heard

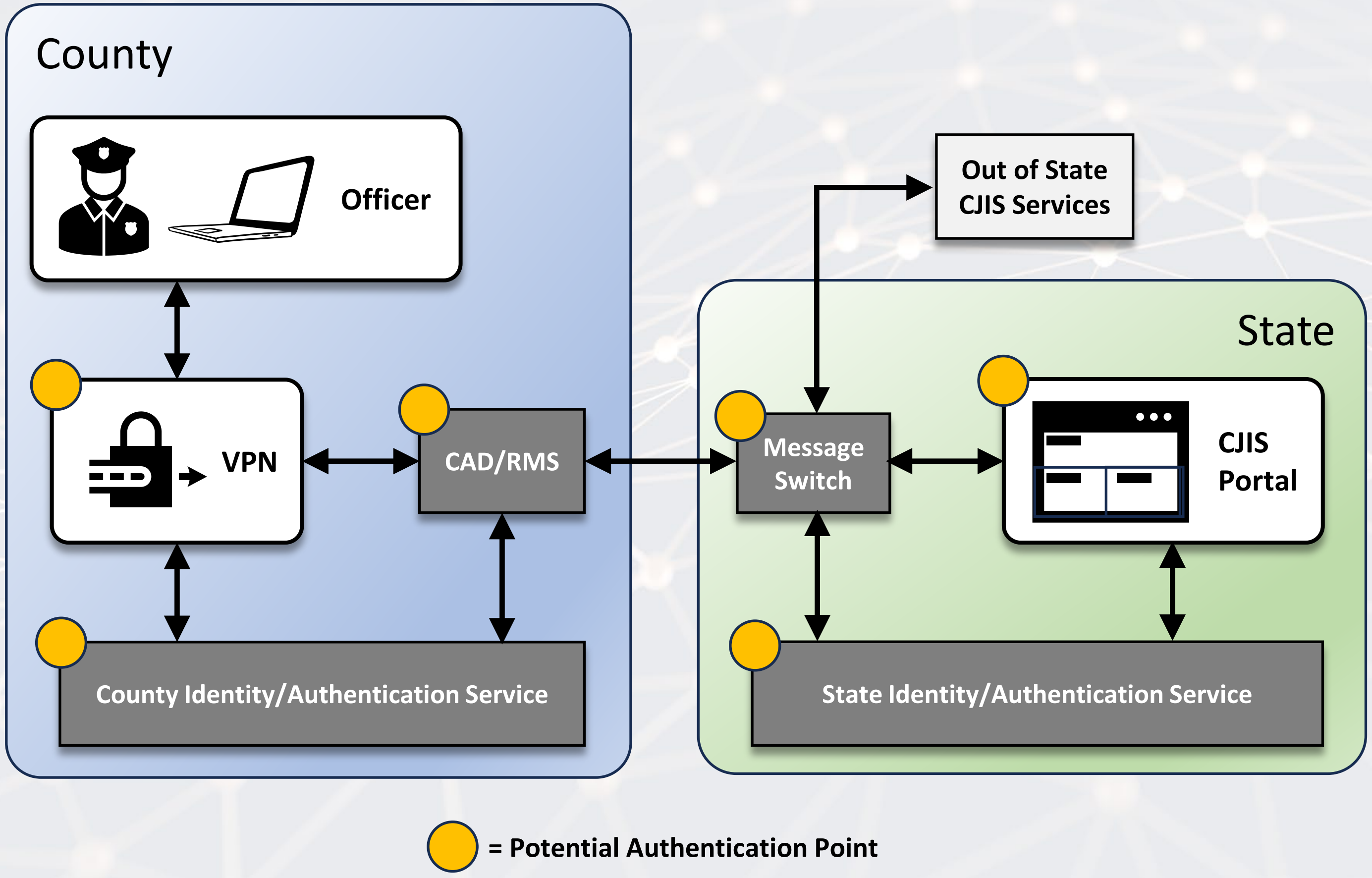
- Common architectural components
- Common ways of accessing CJI
  - State portal
  - CAD/RMS
- Interconnectivity between state and local systems
- MFA likely at state portal
- Local agencies required to have MFA before accessing CAD/RMS


County
Officer
VPN
CAD/RMS
County Identity/Authentication Service
Out of State CJIS Services
State
Message Switch
CJIS Portal
State Identity/Authentication Service

MFA Design Principles

Design Principles Overview

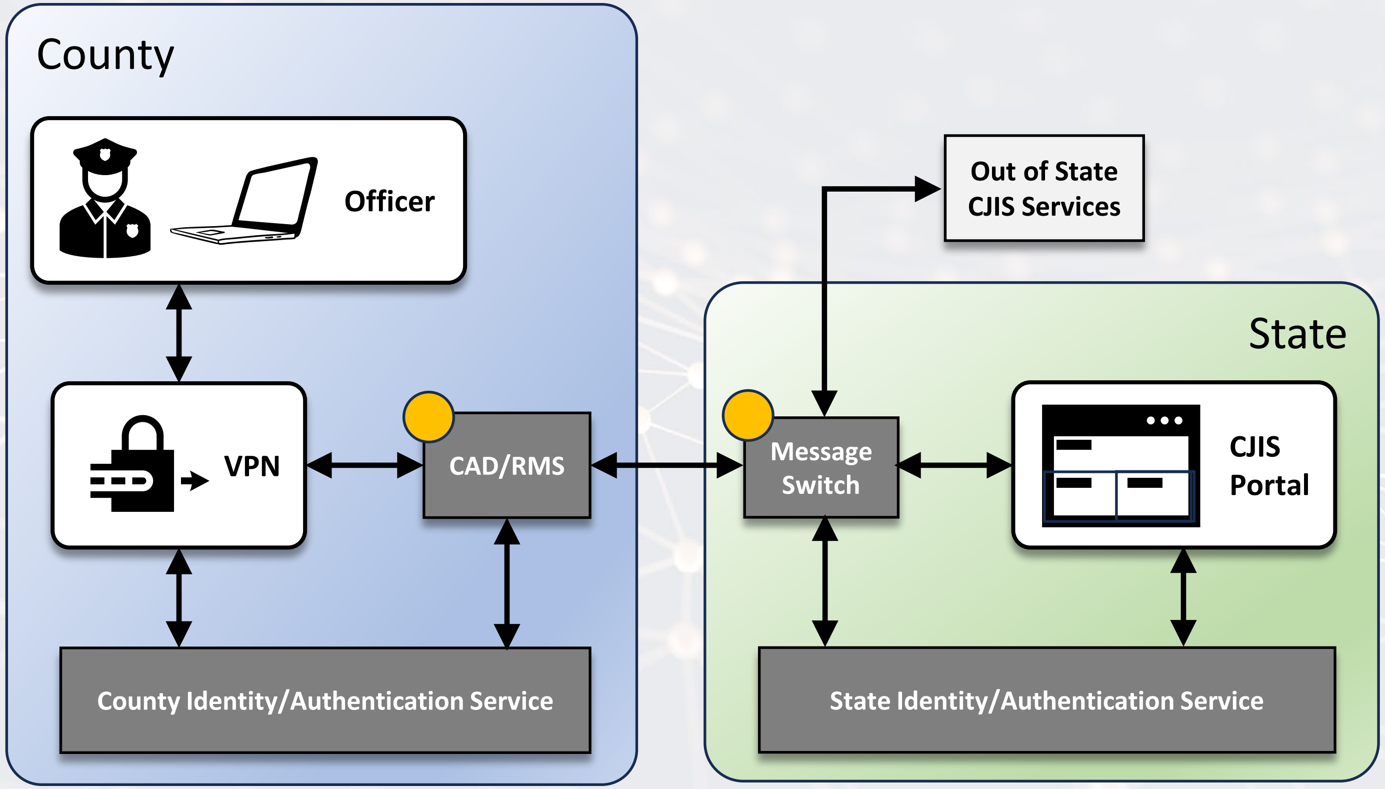
Agencies should consider a few key principles when implementing MFA:


County
Officer
VPN
CAD/RMS
County Identity/Authentication Service
Out of State CJIS Services
State
Message Switch
CJIS Portal
State Identity/Authentication Service
● = Potential Authentication Point

1. **Authenticator re-usability**
2. **Authenticator optionality**
3. **Avoid passing memorized shared secrets**
4. **Ensure MFA is protecting your CJI**

Principle #1: Authenticator Re-Usability

- Minimize the number of credentials users have to manage
- Save money by leveraging pre-existing MFA or identity services which may exist at the state, county or local level, inside or outside of public safety departments
- Challenge: User is required to maintain 2 sets of MFA credentials, one locally for CAD/RMS and another when accessing the state CJIS portal

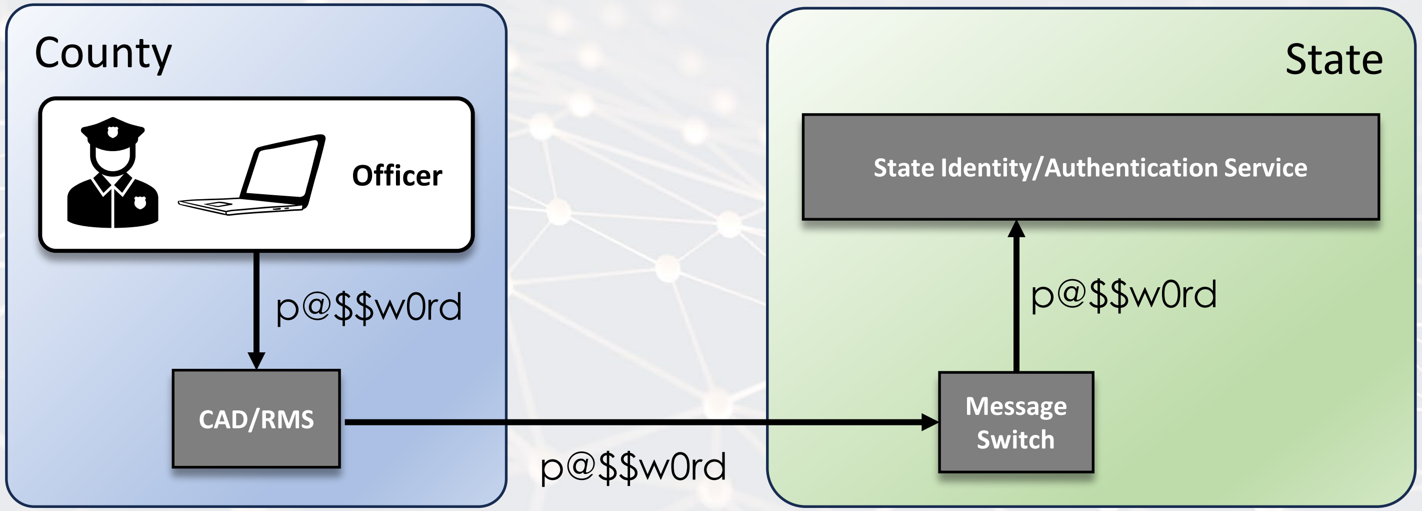


Principle #2: Authenticator Optionality

- Agencies have a diverse set of user authentication requirements.
- Giving agencies authenticator optionality allows them to meet the user needs and use cases.
- Challenge - Department of corrections:
  - Phone not allowed in facility
  - No biometrics available
  - Tokens too costly
  - Users are not assigned to specific devices

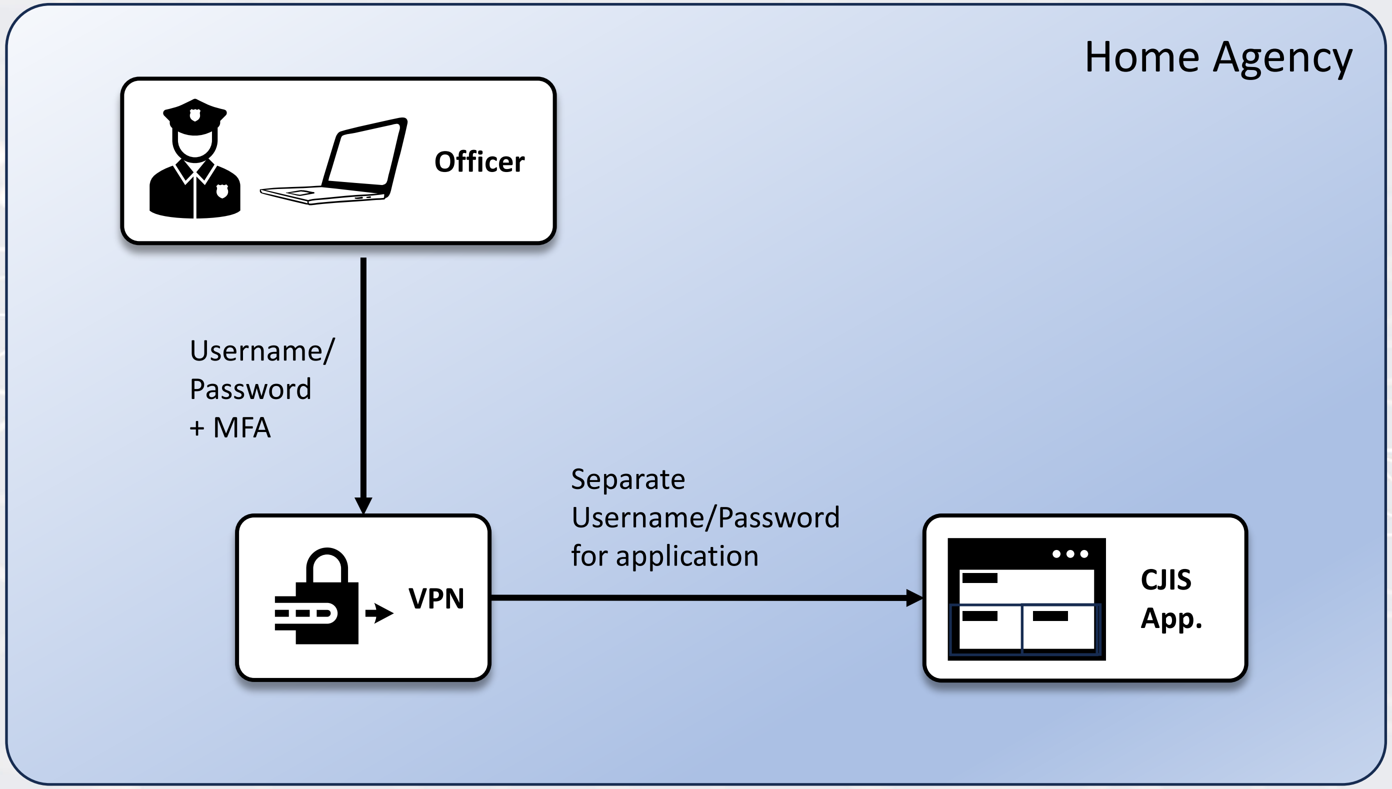
Principle #3: Avoid Passing Memorized Shared Secrets

- The passing of shared memorized secrets, such as passwords, between public safety applications and state message switches is a practice that is sometimes used to allow a state switch to authorize a user before getting access to CJI.
- Security concerns exist with this model. Passing of memorized shared secrets should be avoided to the greatest extend possible.



Principle #4: Ensuring MFA protects CJI

- Just because MFA is “in front” of a CJIS application does not mean it’s providing the intended level of security.
- MFA does not need to be at the application, but it should be integrated with the application.
- Challenge: User authenticates with MFA at a VPN service, but when accessing a CJI application needs a separate username and password.



Because most states have multiple ways to access CJI and access to CJI often requires cross-jurisdictional (across state, local, tribal and territorial) connection between IT systems, implementing these MFA principles can be a challenge.

Supporting Technology

Standards & Best Practices that support MFA

“It Depends” still applies, but in general there are some standards and best practices that if supported by vendors could help agencies implement MFA. Specifically:

1. Identity Federation & other token-based protocols
2. Integration with Identity Services
3. Single Sign-On

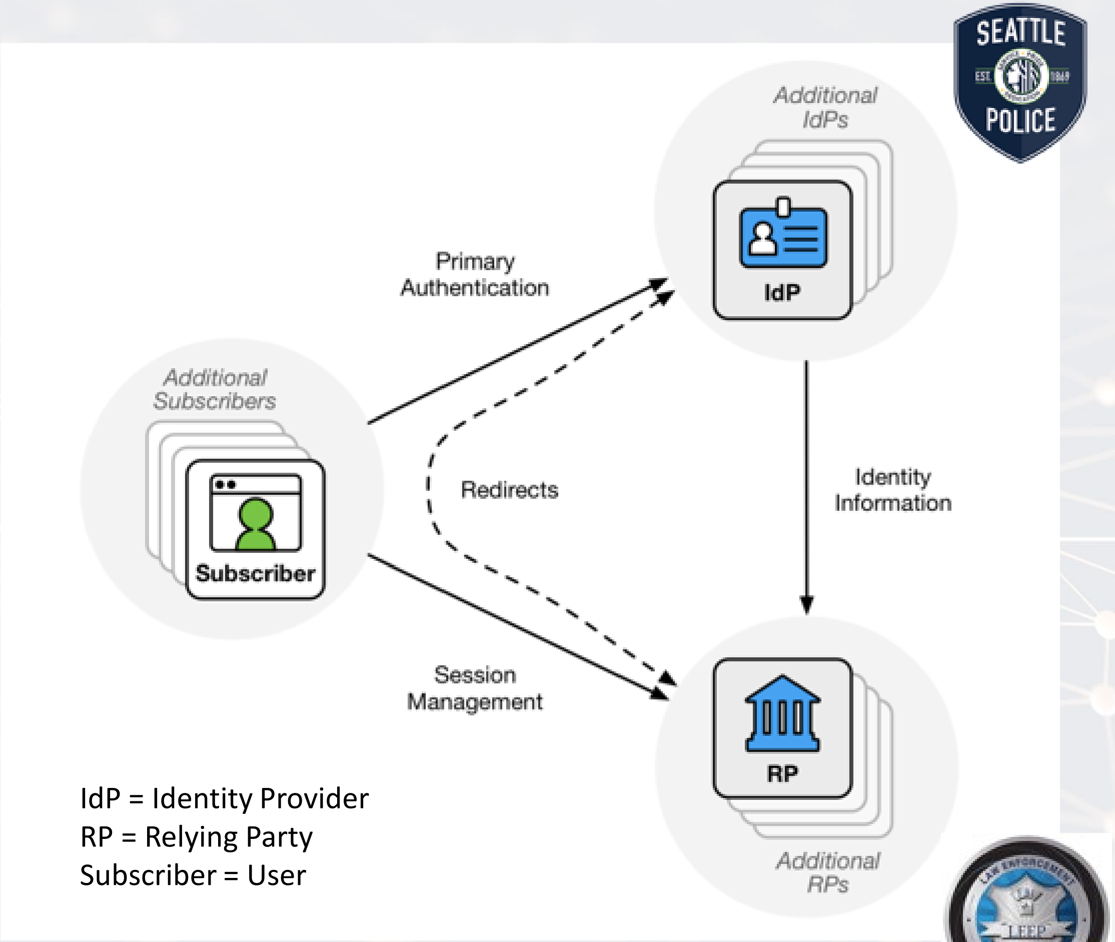
OpenID Connect

SAML v2.0
Security Assertion Markup Language

Identity Federation

- Identity Federation allows for the conveyance of identity and authentication information across a set of networked systems.
- Designed to alleviate the need to pass memorized shared secrets across networks.
- Supports integration between Identity services and applications that need to consume identity information such as authentication success/failure and attributes about the user.
- Two common protocols: OpenID Connect 1.0 and SAML 2.0

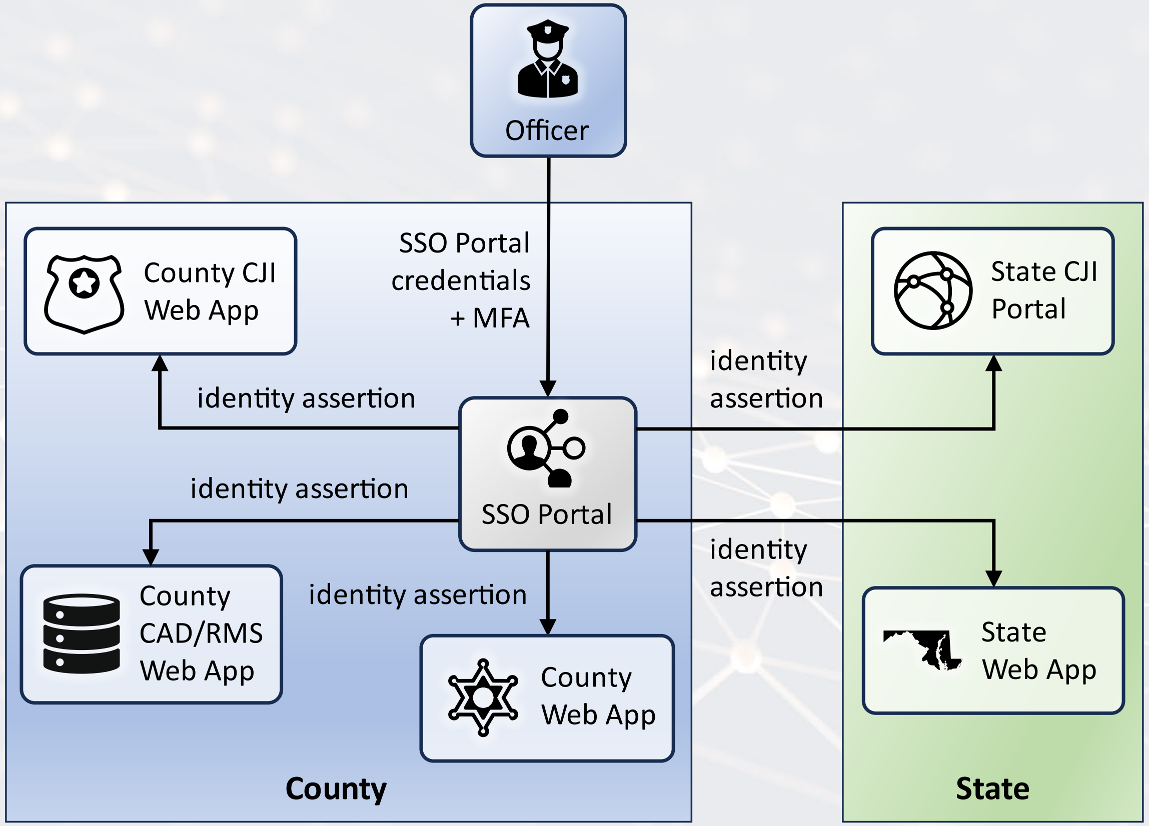
NOTE: Identity Federation is the primary way to support the passing of attributes under the AC-2 control.



IdP = Identity Provider
RP = Relying Party
Subscriber = User

Integration with Identity Services

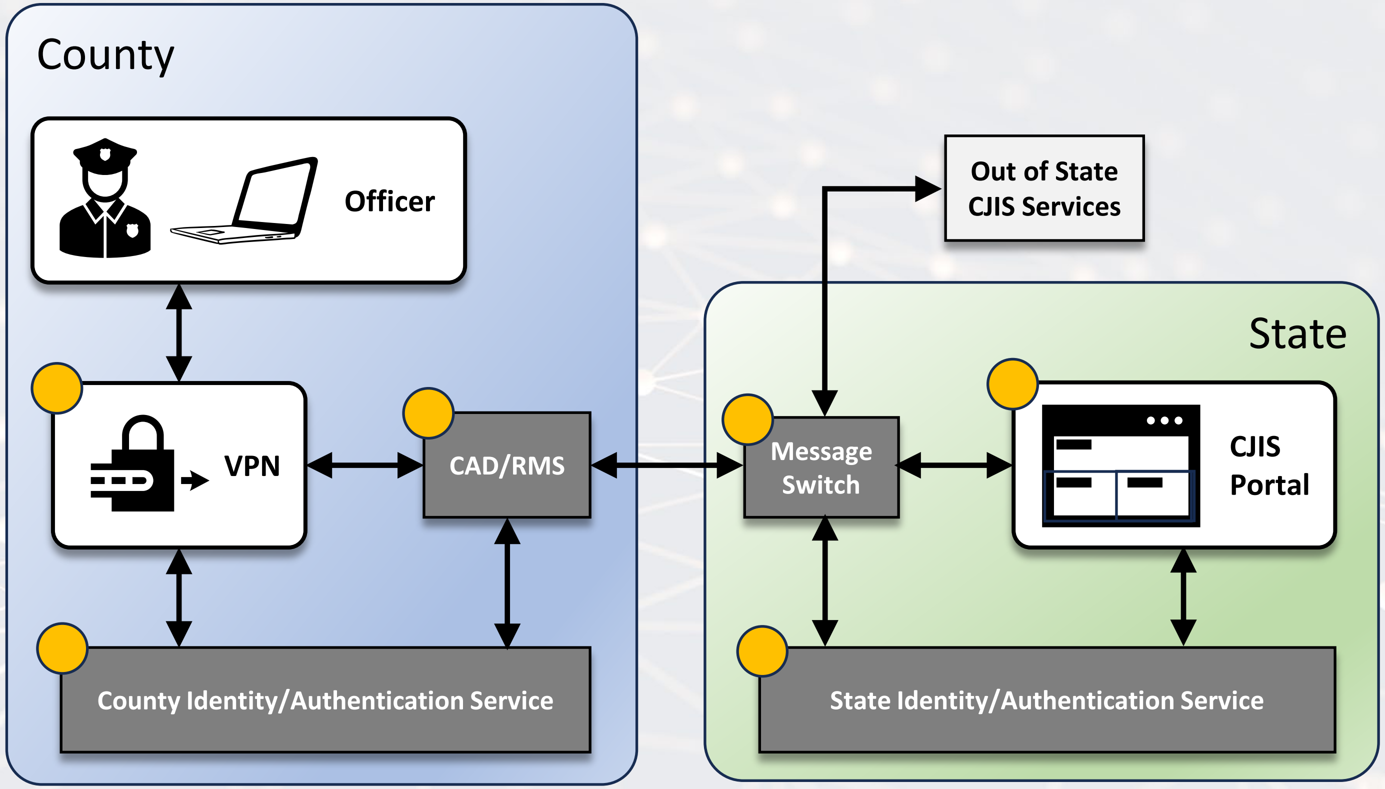
- Dedicated identity services provide several potential benefits:
  - Alleviate the need for other applications to manage user IDs and credentials
  - Identity services often support all major identity protocols and authentication methods
  - Can enable SSO models to reduce the number of credential users need to manage
  - Identity services can be centralized and enable shared service models and/or cost savings



Example of CJIS application behind an SSO service

Example Use Cases

Commonly seen State and Local CJI Architecture


County
Officer
VPN
CAD/RMS
County Identity/Authentication Service
Out of State CJIS Services
State
Message Switch
CJIS Portal
State Identity/Authentication Service

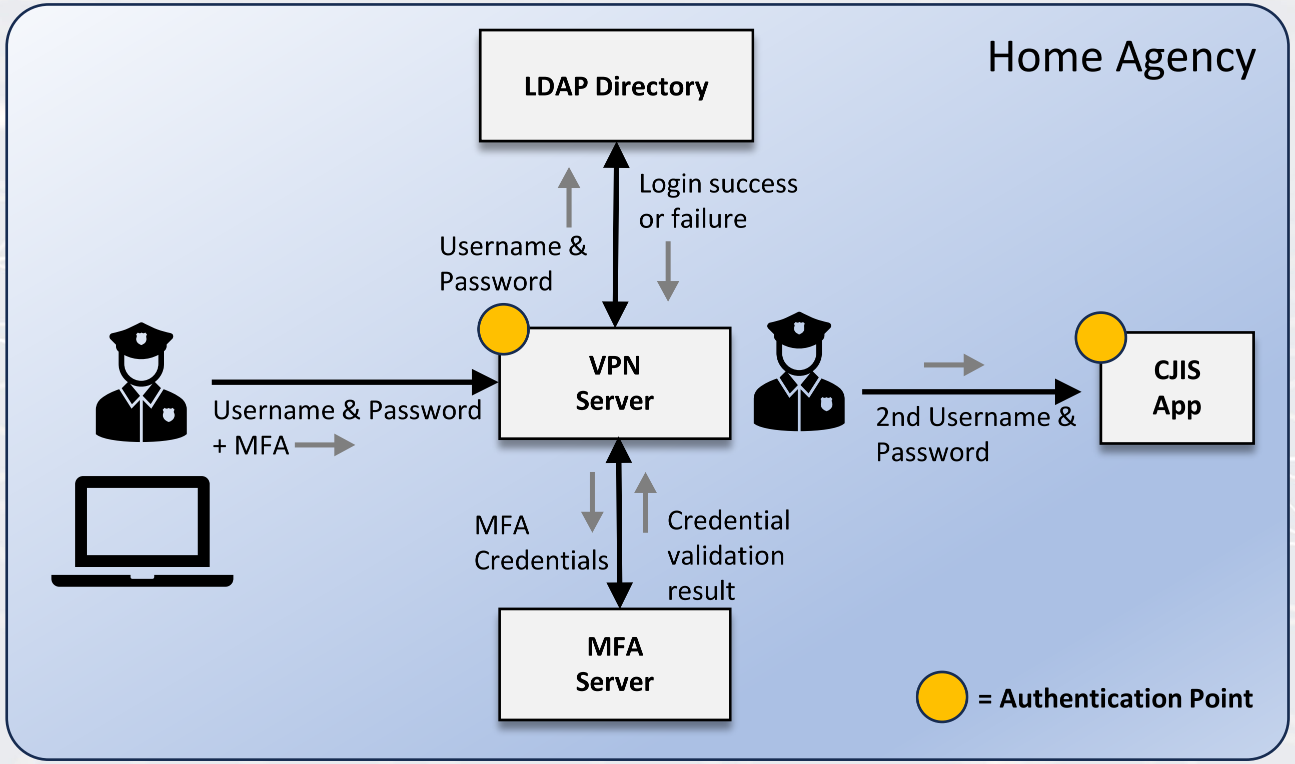
● = Potential Authentication Point

Any of the orange dots are reasonable places to implement MFA. However, each comes with potential trade offs against the 4 MFA principles. The tradeoffs chosen will depend on the requirements of individual organizations. The following slides highlight use cases we have seen and ways to implement MFA for those use cases using standards and best practices.

VPN Use Case

VPN Use Case

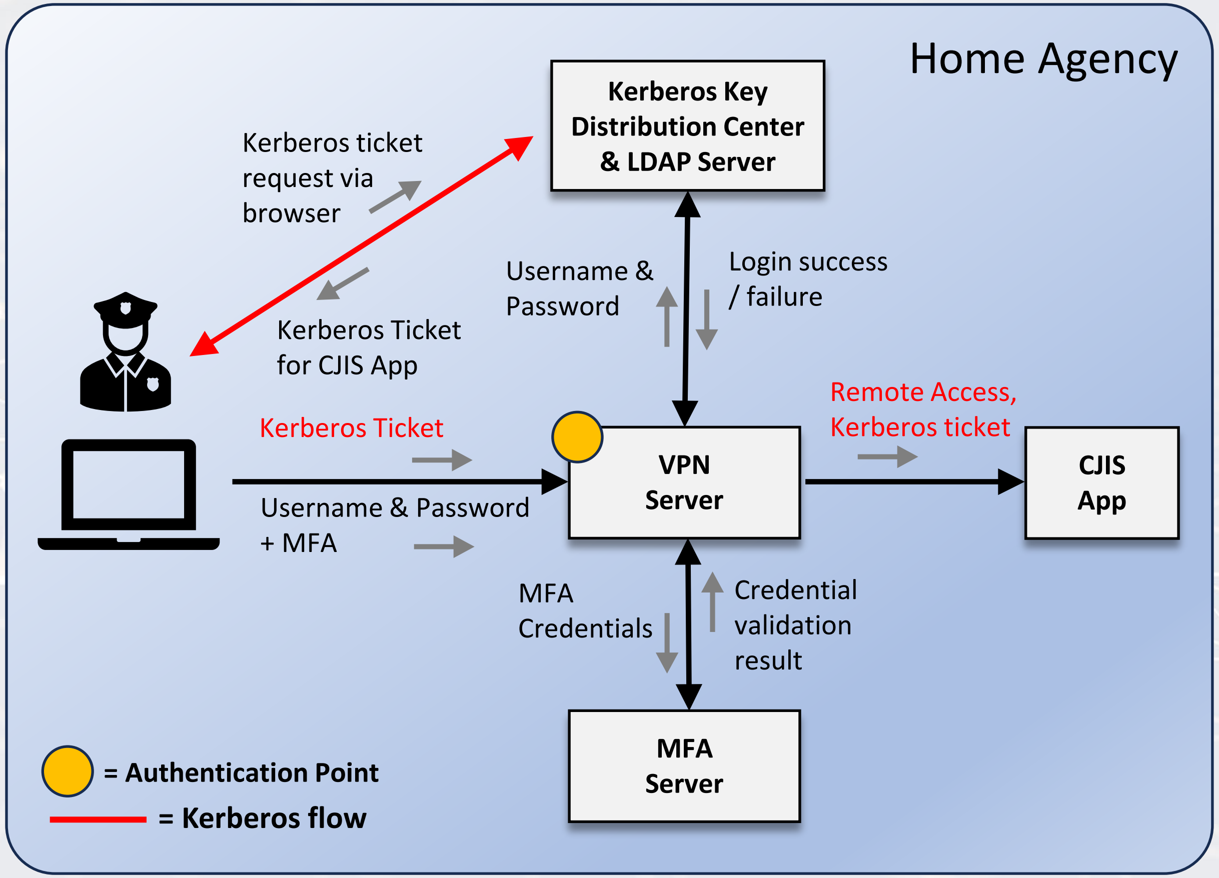
- Implementing MFA at the VPN is a very viable option, but not all implementations are equal.
- In this example, the user authenticates with MFA at a VPN service, but when accessing a CJI application they need a separate username and password.
- In this design MFA is "in front" of the CJIS application, yet the application is still left open to Phishing or Password database breaches.
- Plus, the user has to input and manage a second credential.
- Recall principles #1 and #4



Example when MFA is not integrated with the CJIS application

VPN Use Case with Kerberos

- As mentioned previously a token-based system could help alleviate this. This example shows a Kerberos-centric architecture.
- Once the user successfully authenticates to the VPN service with their MFA credentials, rather than providing a second username and password to the CJIS application, the user's browser gets redirected back to the LDAP service and is given a Kerberos ticket that can be presented by the browser to access the CJIS application.
- Benefits:
  - User no longer needs to manage a second credential
  - Kerberos tickets are not phishable
  - No need for a password database associated with the CJIS app.

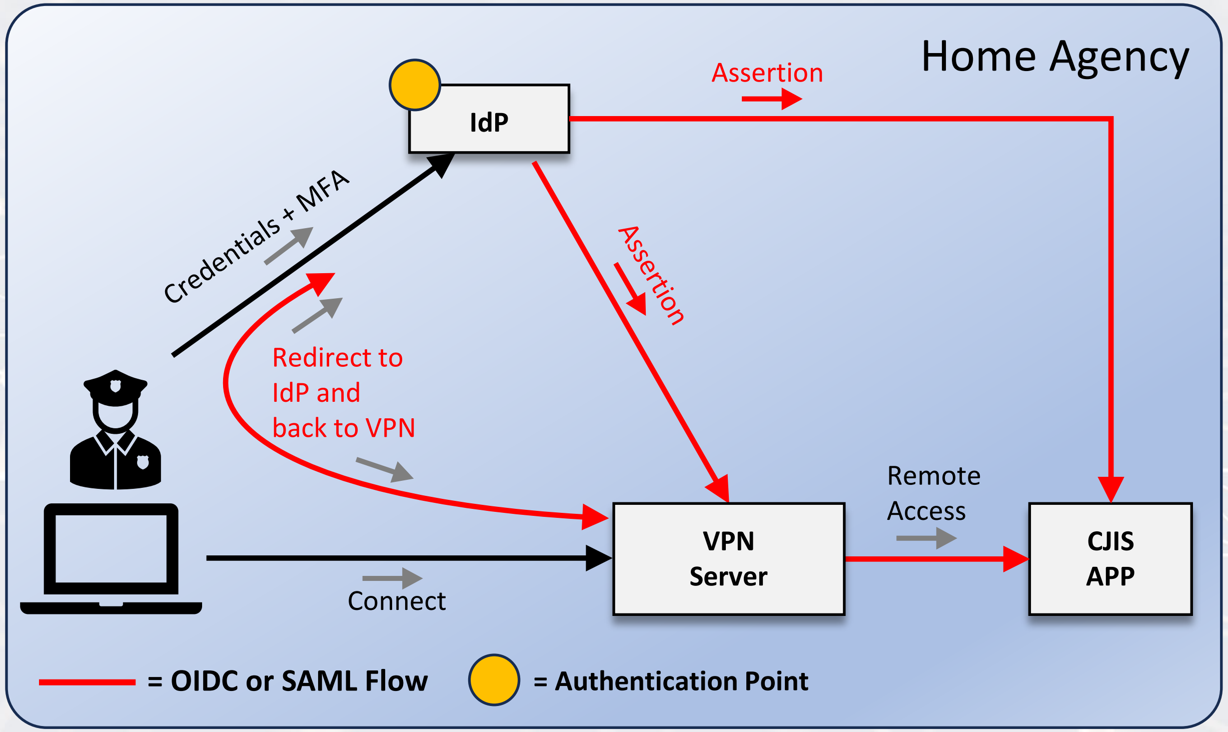


Home Agency
Kerberos Key Distribution Center & LDAP Server
Kerberos ticket request via browser
Kerberos Ticket for CJIS App
Username & Password
Login success / failure
Remote Access, Kerberos ticket
Kerberos Ticket
Username & Password + MFA
VPN Server
CJIS App
MFA Credentials
Credential validation result
MFA Server
= Authentication Point
= Kerberos flow

Example of how MFA at the VPN could be integrated using Kerberos

VPN Use Case with Federation

- Similar to Kerberos, federation protocols like OIDC and SAML can be used.
- In this scenario the user authenticates at the IDP and is given an assertion, an OpenID or SAML token, that can be given both to the VPN service and the CJIS App.
- Benefits:
  - User no longer need to manage a second credential
  - SAML/OIDC tickets are not phishable
  - No need for a password database associated with the CJIS app.

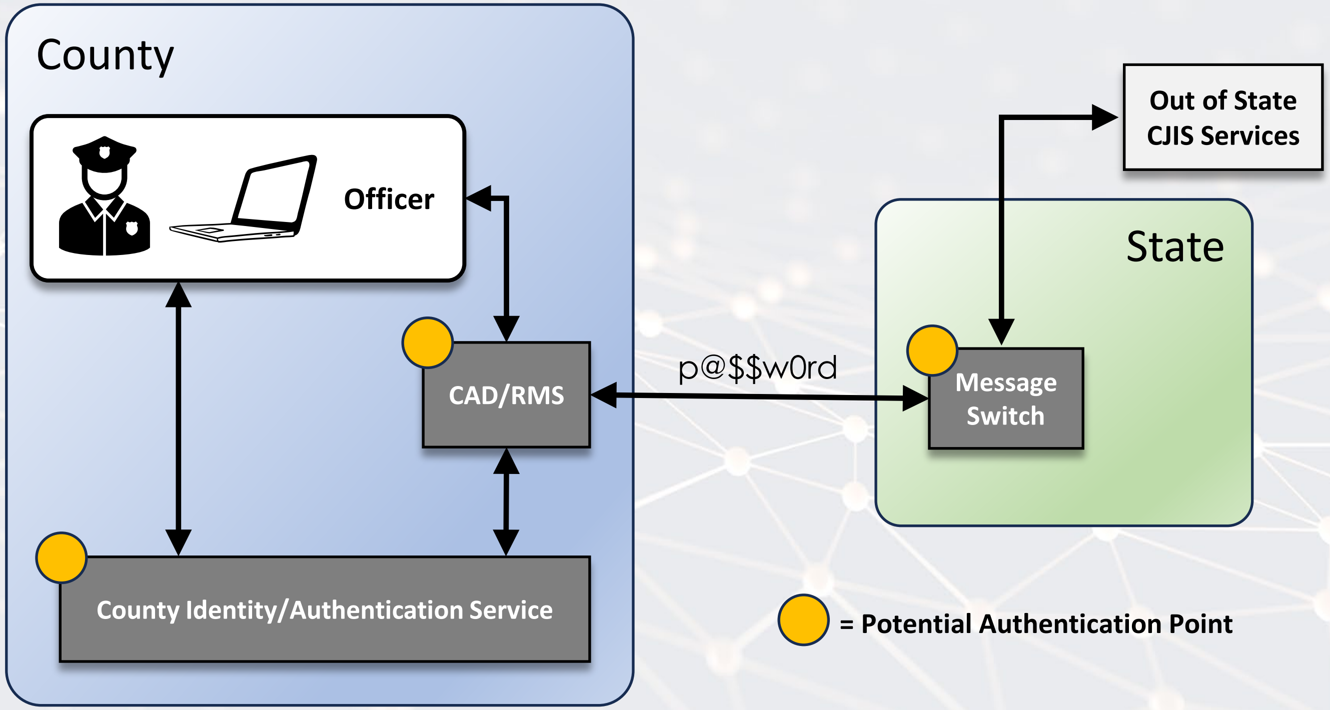


Example of how MFA at the VPN could be integrated using SAML or OIDC

Local Agency Use Case

Common MFA implementations for Local Agency

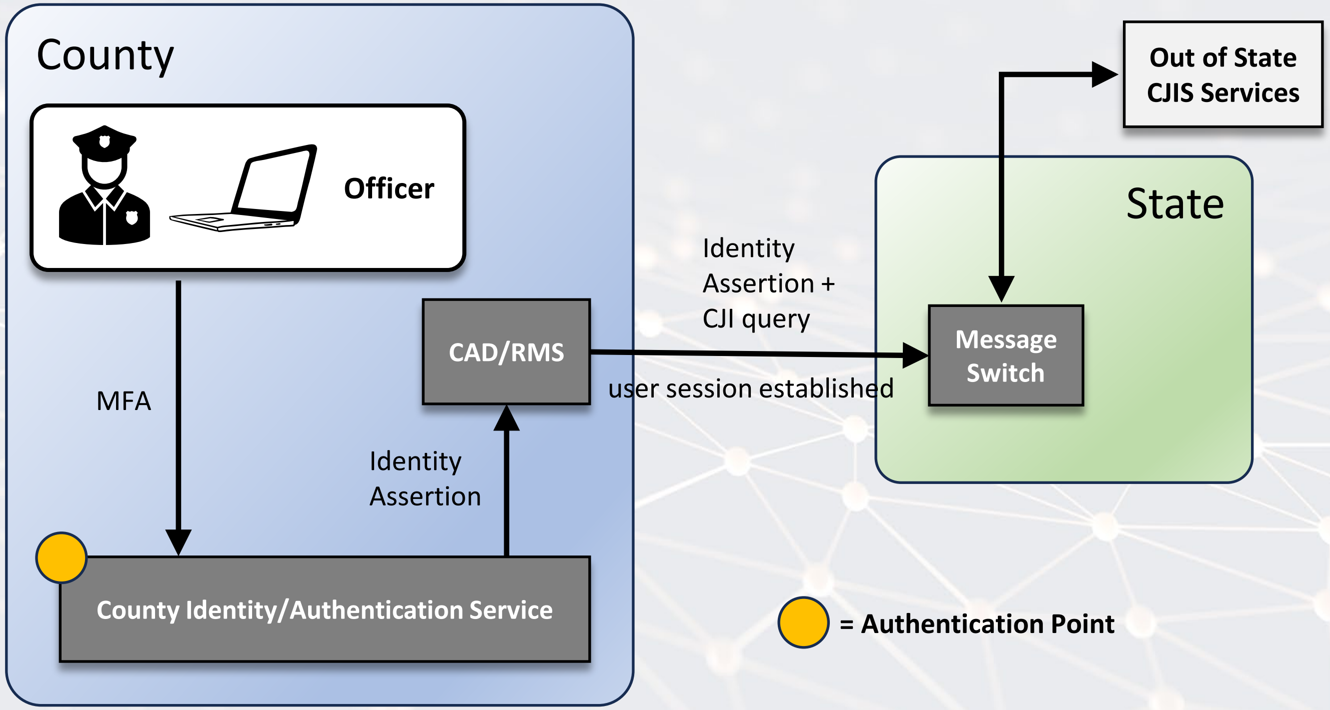
- MFA integrated at message switch:
  - May not have MFA optionality
  - MFA likely cannot be reused
- MFA integrated at the CAD/RMS
  - May not have MFA optionality
  - MFA likely cannot be reused
  - Identity information needs to be passed between CAD/RMS and Message Switch
- MFA at local Identity service
  - Likely to have more MFA optionality
  - MFA can likely be reused
  - Identity information still need to be passed to other applications


County
Officer
CAD/RMS
County Identity/Authentication Service
p@$$w0rd
Out of State CJIS Services
State
Message Switch
= Potential Authentication Point

Simple but common architecture of how local agencies access CJI

Potential MFA implementations for Local Agency

- MFA integrated at local agency identity service to maximize authenticator optionality and re-useability
- Federation protocols use to integrate MFA with CAD/RMS
- Federation protocols allow for the sharing of identity information between CAD/RMS and message switch without sharing passwords.

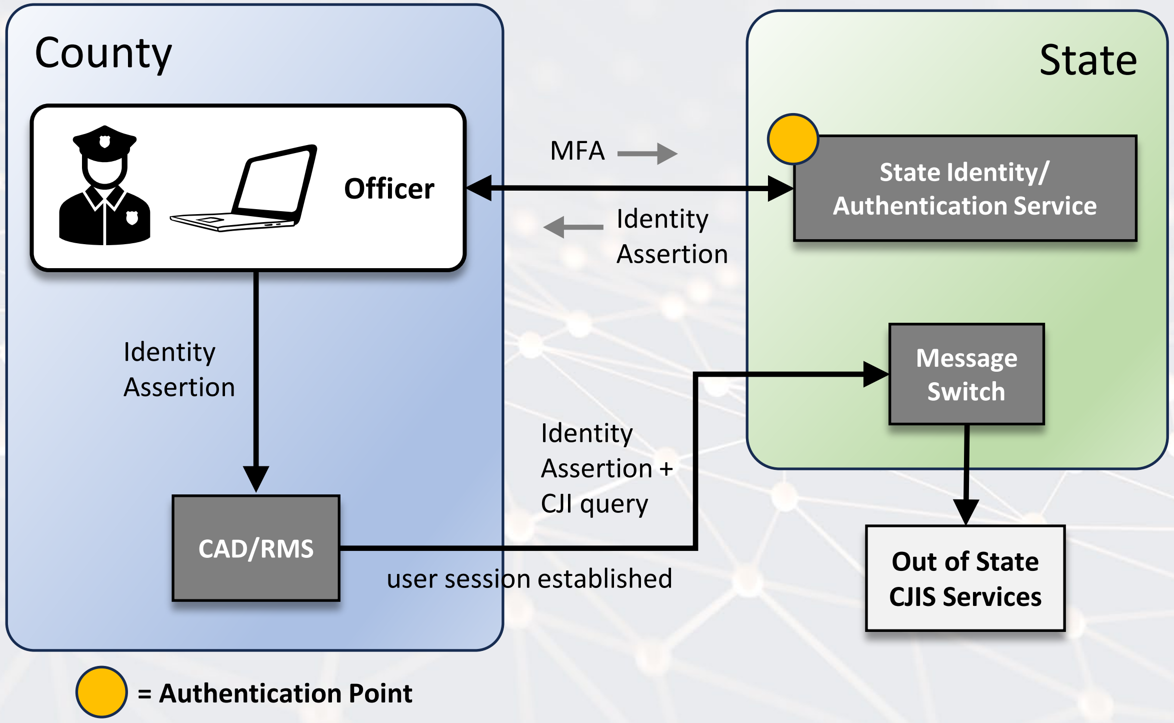


County IDP integrated with CAD and RMS using Identity Federation

NOTE: This requires CAD/RMS and Message switch vendors to support federation protocols.

Potential State IDP for Local Agency

- In this model the state agency IDP is an identity service that can offer local agencies MFA capabilities
- Similar to the last model integrating with identity service typically offers maximum MFA optionality and re-usability
- This model could be good for small and rural agencies who cannot implement their own MFA
- This could also enable a shared service model where the state acting as IDP could save on costs and MFA implementation variation across the state



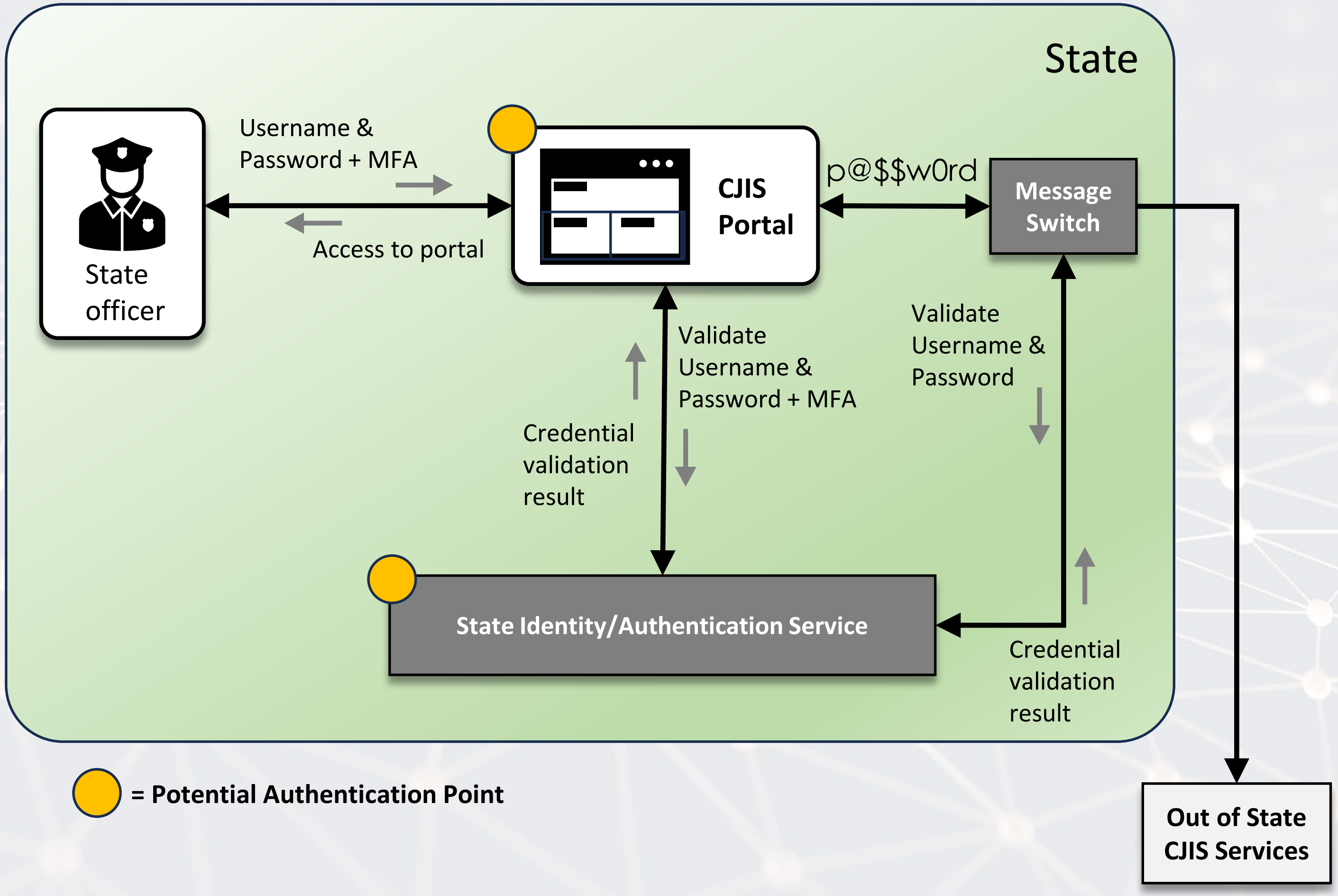
State IDP integrated with Local CAD and RMS using Identity Federation

NOTE: This requires CAD/RMS and Message switch vendors to support federation protocols.

State Agency Use Case

Common State Portal Deployment

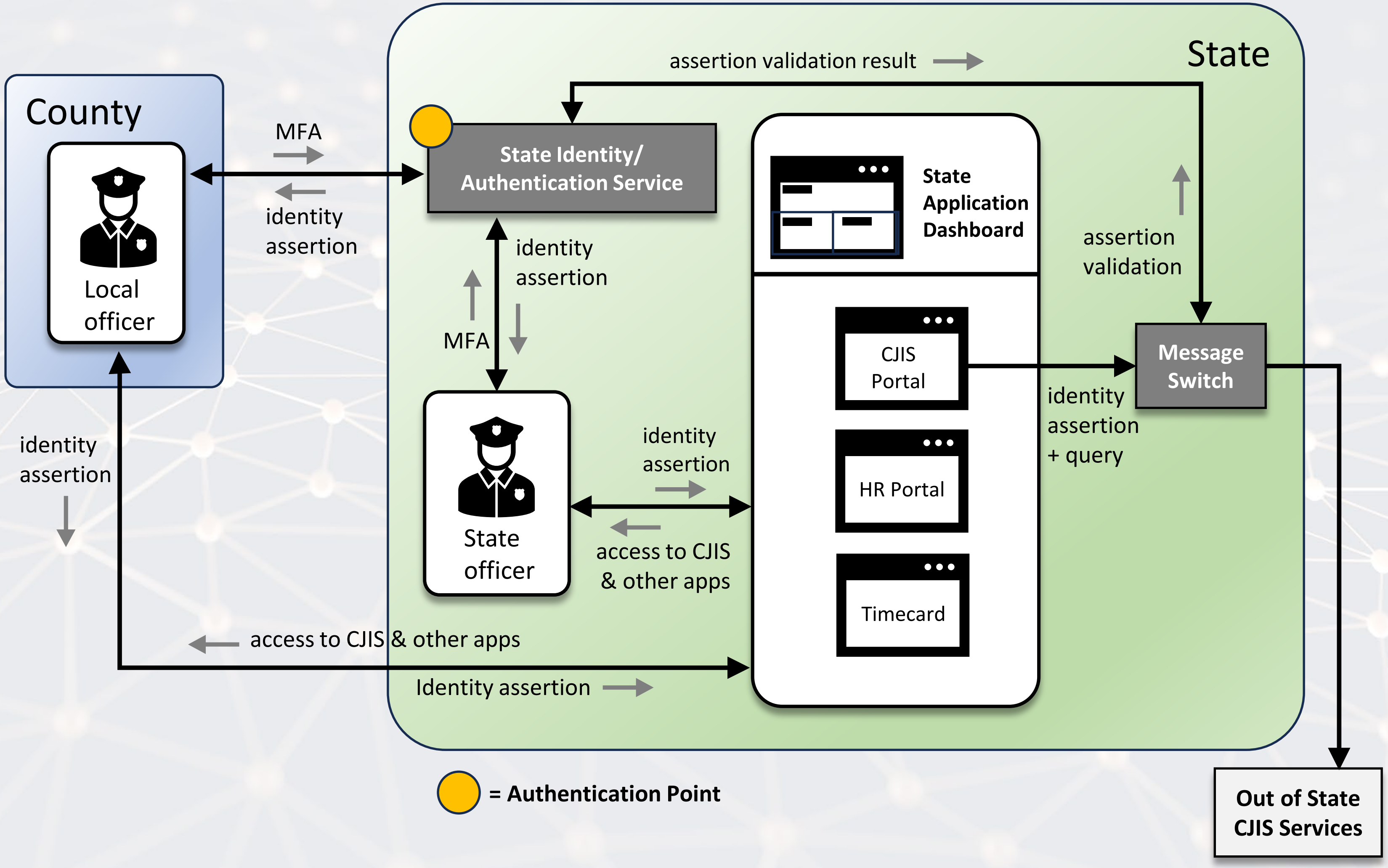
- MFA integrated at the state portal:
  - May not have MFA optionality
  - MFA likely cannot be reused
- MFA integrated at the state identity service:
  - Likely to have more MFA optionality
  - MFA can likely be reused
  - Identity information still need to be passed to other applications
- With this model we’ve still seen the need to pass a password to the state switch for verification.


State
State officer
Username & Password + MFA
Access to portal
CJIS Portal
p@$$w0rd
Message Switch
Validate Username & Password + MFA
Credential validation result
Validate Username & Password
State Identity/Authentication Service
Credential validation result
Out of State CJIS Services

● = Potential Authentication Point

Potential State Portal Deployment

- Diagram shows state CJIS portal integrated with an application dashboard accessible via state and local users authenticating at the state identity service
- Many organizations have this type of dashboard. It could be leveraged for CJIS applications
- The dashboard vendors are usually also identity service vendors that support federation protocols and many different types of authentication
- Putting multiple applications, both CJI and Non-CJI enables single sign-on and minimizes the number of credentials users need to manage



NOTE: This requires CAD/RMS and Message switch vendors to support federation protocols.

Questions & Discussion

Call to Action

- Whether you’re a vendor or agency consider the MFA implementation principles.
- We would love to see more support amongst public safety technology for the protocols we’ve talk about in this presentation.
- This mission space is important and we all have a role to play in MFA implementation.
- There is business value to be had by vendors and agencies alike.

PULLING THE FUTURE FORWARD

Contact Us

Email us: ps-mfa@list.nist.gov

Join our community of interest and get updates on our work:
https://www.nccoe.nist.gov/public-safety-first-responder