Current Cyber Threats and What's the Best Way to Keep Current

Utah TAC Conference

September 14, 2022

Jeff Campbell, FBI CJIS Deputy ISO

Discussion Topics

- **Cyber Threat Trends**
- **Incident Response Capability**
- **Modernized IR Overview**
- **FBI CJIS ISO Resources**

Cyber Threat Trends

Cyber Threat Trends

- **Definitions**
- **Trending Threats**

Definitions

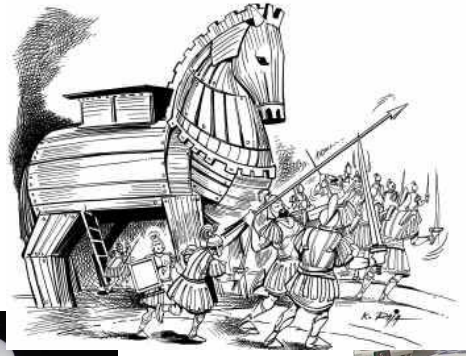
- **Event: any observable occurrence in a system or network (NIST)**
- **Incident: violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (NIST)**
- **Breach: unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to see the information (US-CERT)**

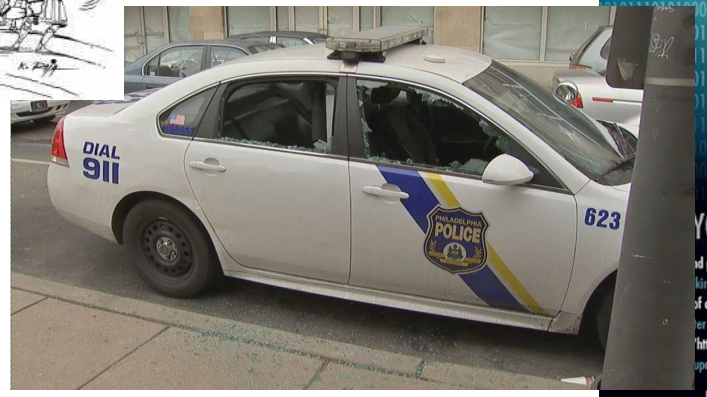
Definitions

- **Incident Response: technical actions taken during an incident**
- **Incident Handling: management actions taken during an incident**

What is a security incident?

Any security event involving CJI



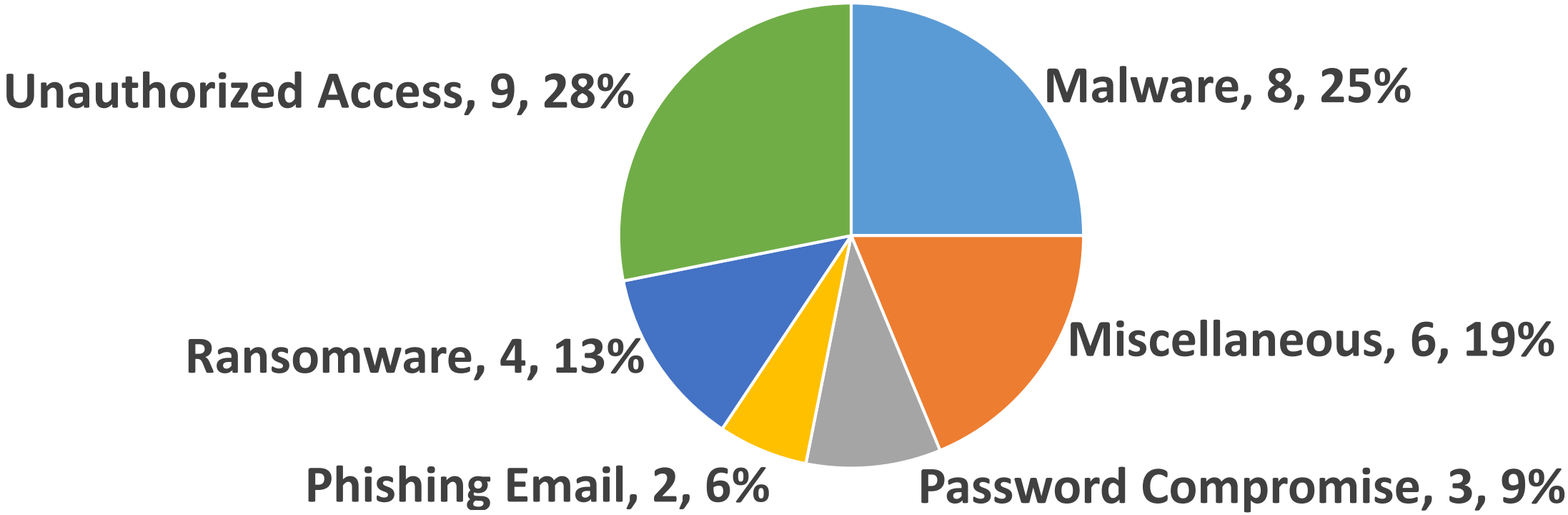


Trending Threats

- Since 2012
- ~24 States Reporting
- ~150 Incidents

Trending Threats

2021: 32 incidents reported to FBI CJIS ISO



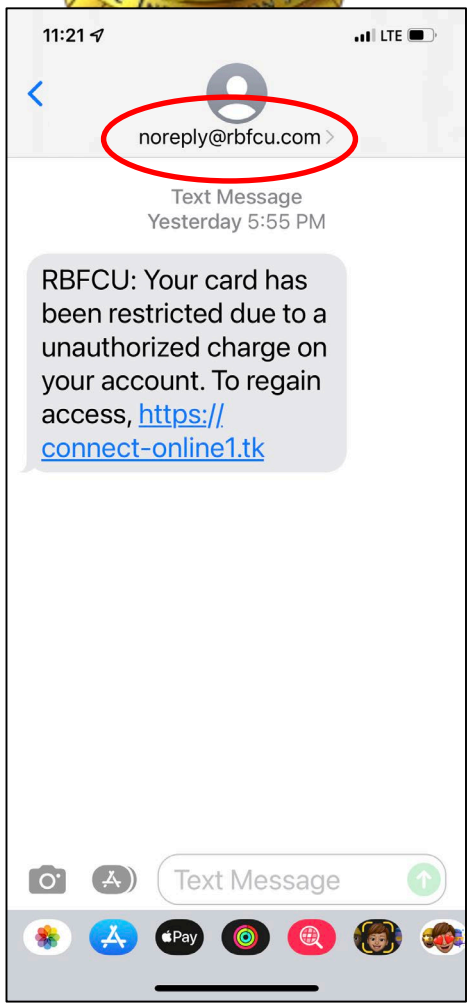
Trending Threats

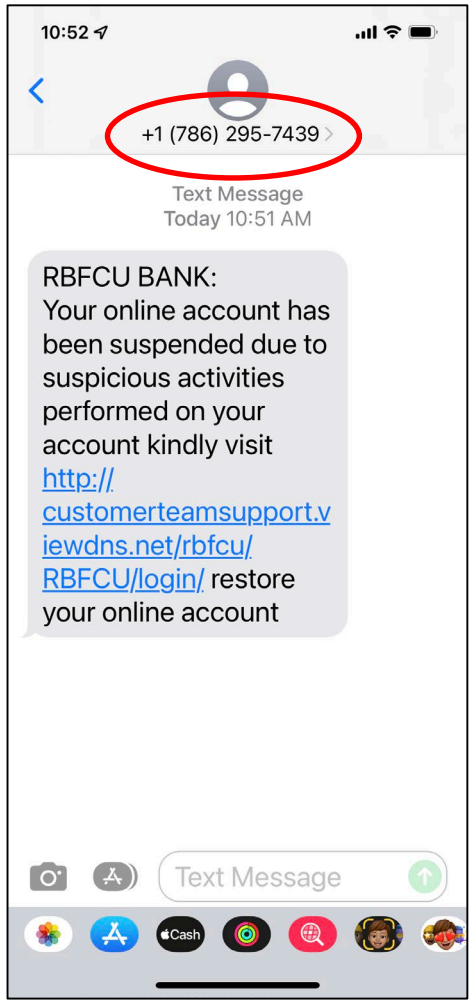
- **Unauthorized Access**
  - Physical
  - Logical
- **Malware**
  - Trojans
- **Ransomware**

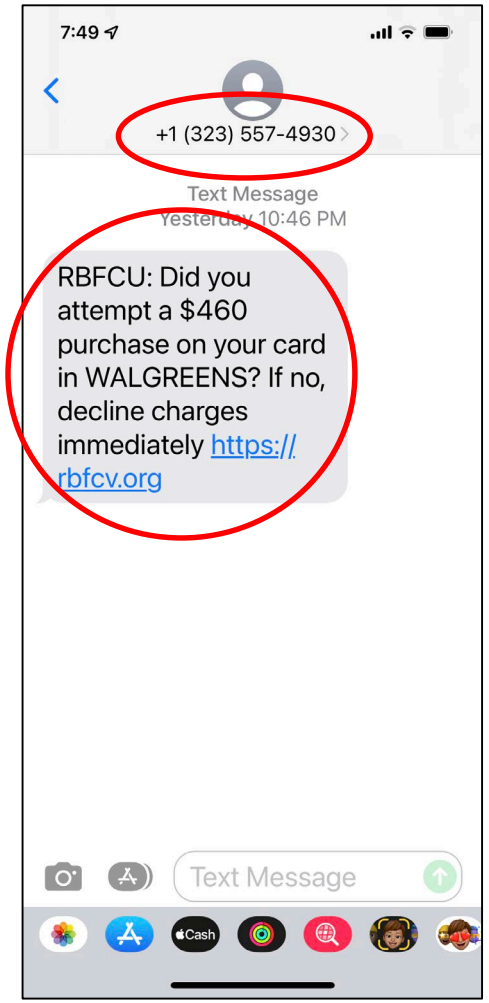
Compromise Methods

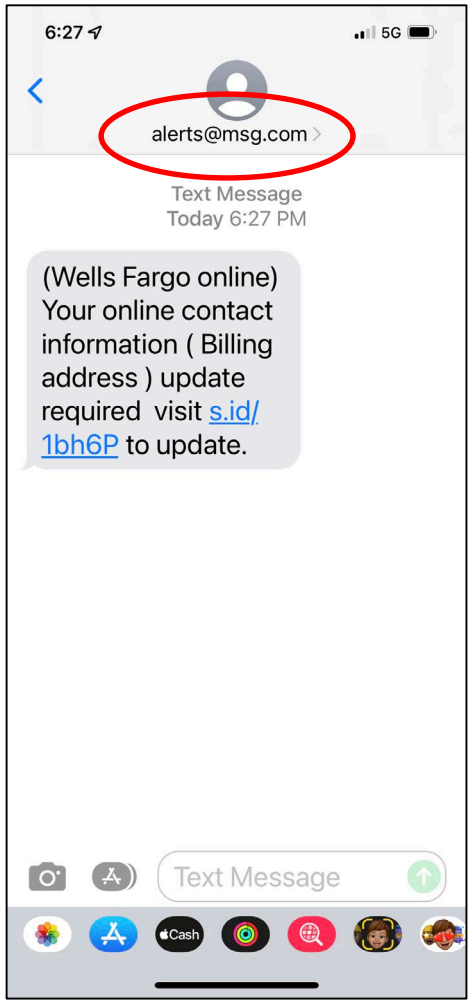
- **Unauthorized Access**
  - Social engineering
  - “Rogue” devices
- **Malware**
  - Outdated antivirus definitions
  - Default passwords
- **Ransomware**
  - Web popups
  - Phishing/Smishing email

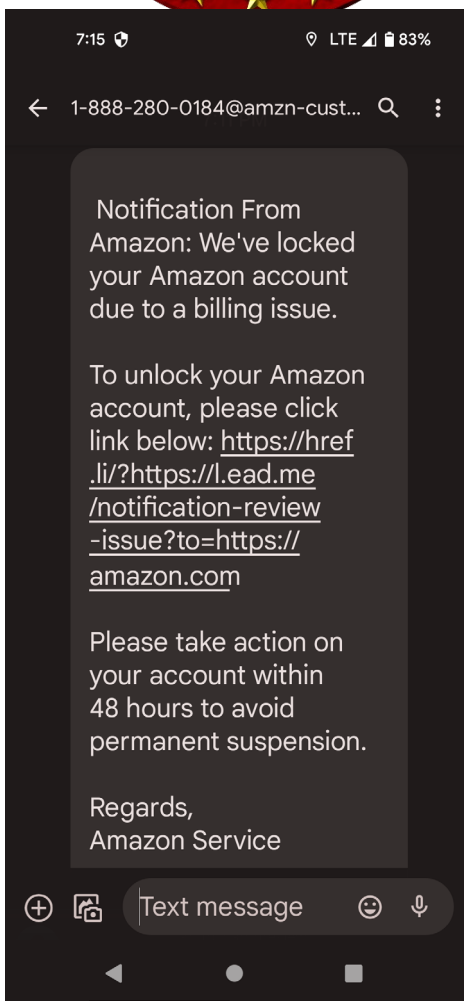
Compromise Methods











Mitigation Methods

- **Unauthorized Access**
  - Audit logs
  - Policies, rules of behavior
- **Malware**
  - Updated antivirus definitions
  - Changing default passwords
- **Ransomware**
  - Updated antivirus definitions
  - Backups

Mitigation Methods

Training

- Types of events and weaknesses
- Roles & responsibilities
- Testing procedures
  - Review
  - Tabletop exercises

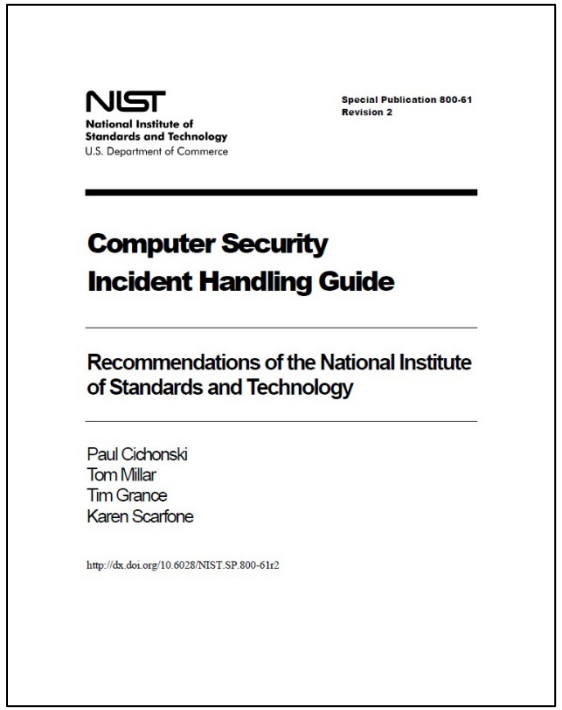
Incident Response Capability

AKA – What's the Best Way to Keep Current

Incident Response Capability

NIST Incident Handling Guidance

- SP 800-61r2, Computer Security Incident Handling Guide
- SP 800-184, Guide for Cybersecurity Event Recovery


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

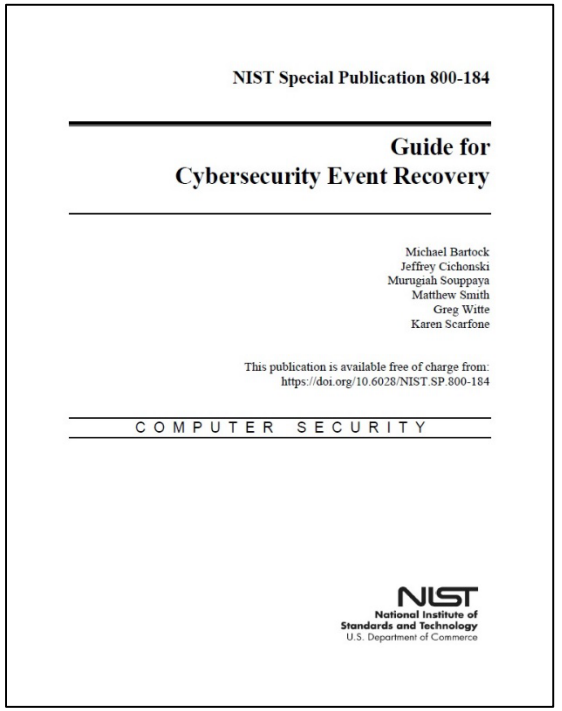
Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2


NIST Special Publication 800-184

Guide for Cybersecurity Event Recovery

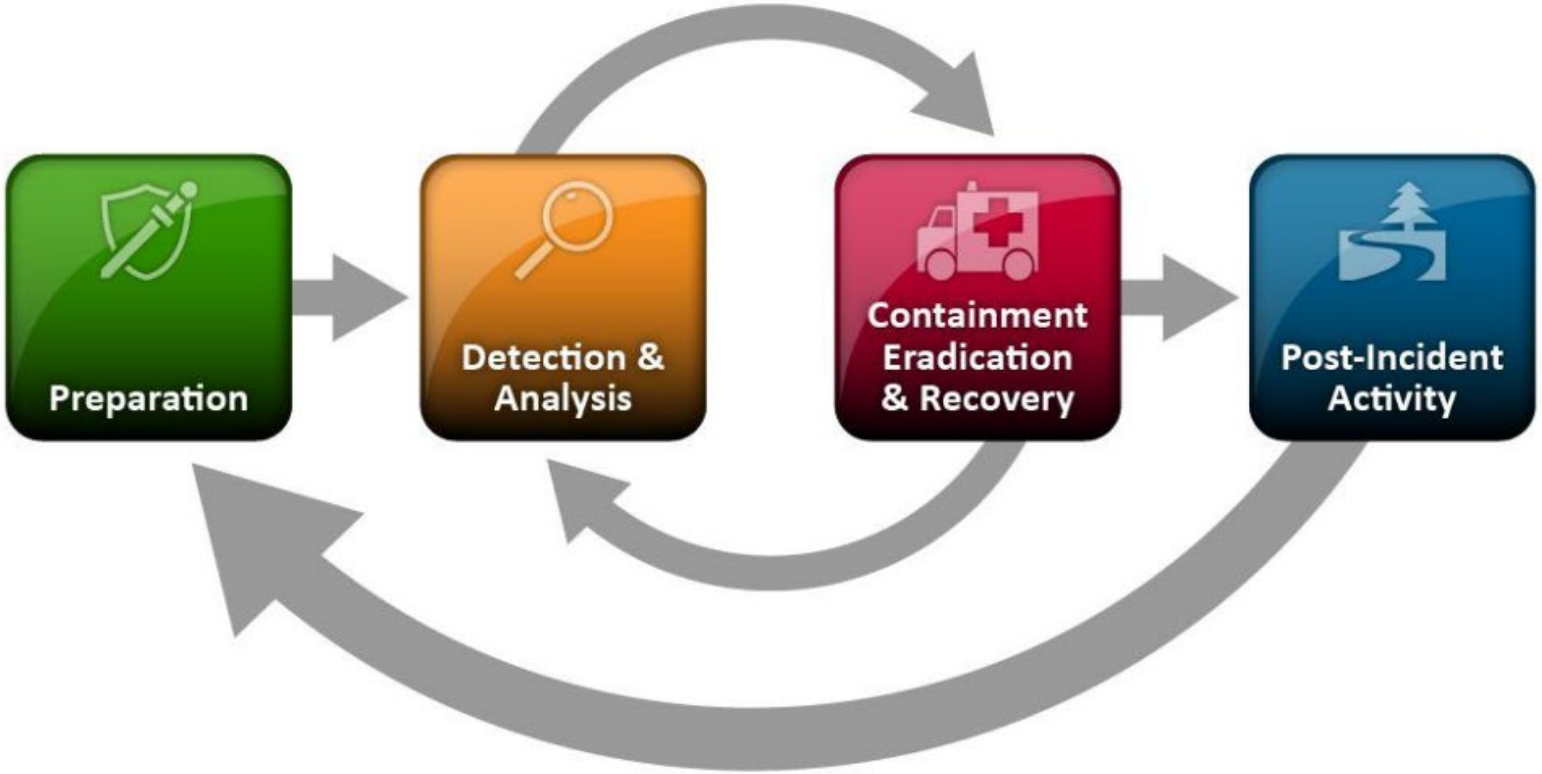
Michael Bartock
Jeffrey Cichonski
Murugiah Souppaya
Matthew Smith
Greg Witte
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-184

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Incident Response Capability



Incident Handling Lifecycle

Incident Response Capability

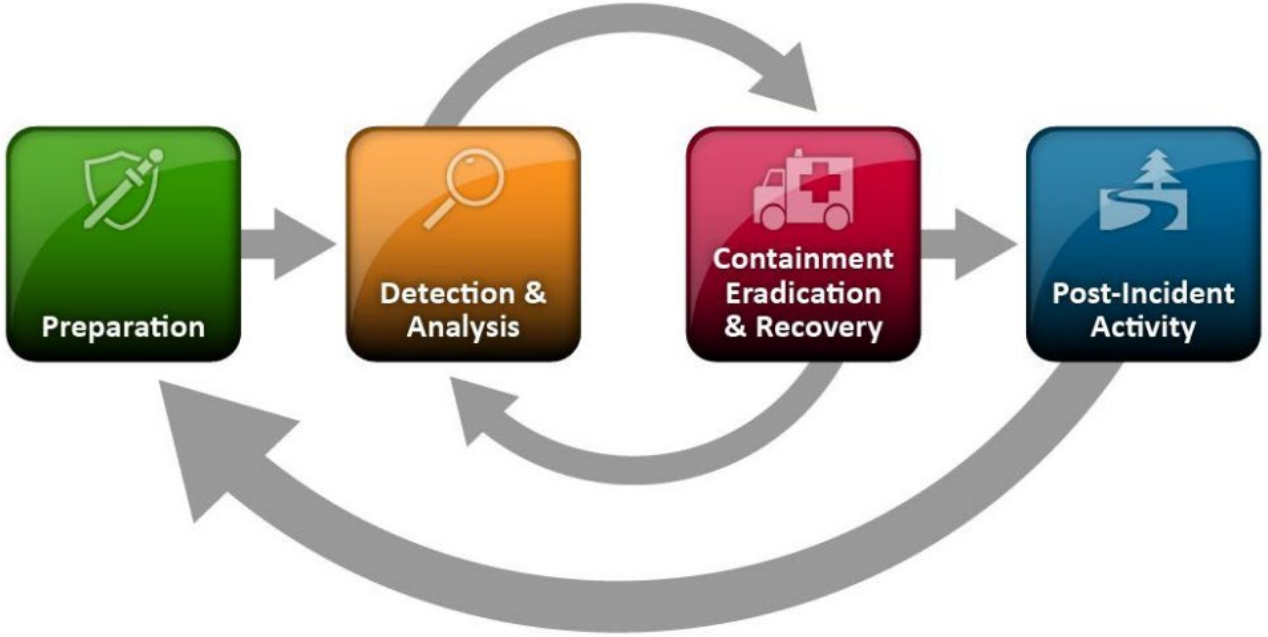
NIST Incident Handling Guidance Should include the following areas:

- Create an incident response policy and plan ✓
- Develop procedure for incident handling/reporting ✓
- Set guidelines for external communications ✓
- Set team structure and staffing ✓
- Establish relationships/comm's with other groups ✓
- Determine response team services ✗
- Staff and train team members ✓

Incident Response Capability

CJIS Security Policy Section 5.3 Policy Area 3: Incident Response

- **(i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery and user response activities**

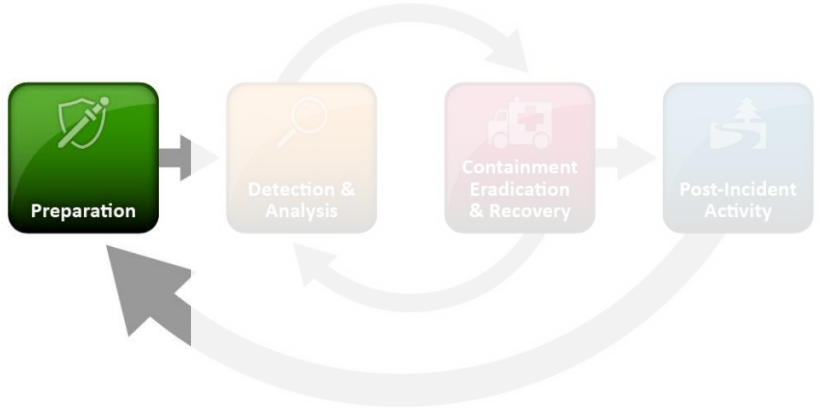


Incident Response Capability

CJIS Security Policy Section 5.3 Policy Area 3: Incident Response

- **(ii) track, document, and report incidents to appropriate agency officials and/or authorities**

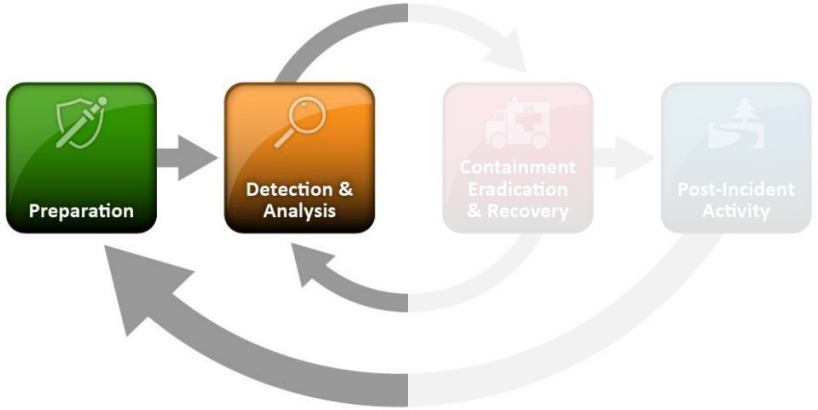
Incident Response Capability



Preparation

- Risk assessment
- Host Security
- Network Security
- Malware Prevention
- User Awareness and Training
- Assigned Roles/Responsibilities
- Communications

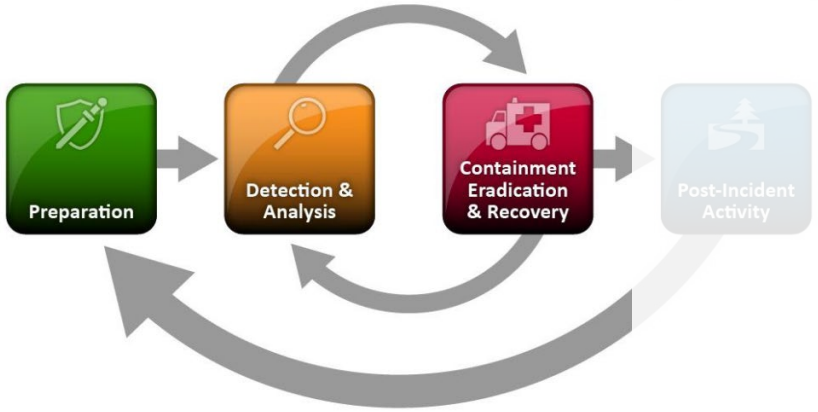
Incident Response Capability



Detection & Analysis

- Attack Vectors
- Signs of an Incident
- Sources of Precursors and Indicators
- Documentation
- Prioritization
- Notification/Communications

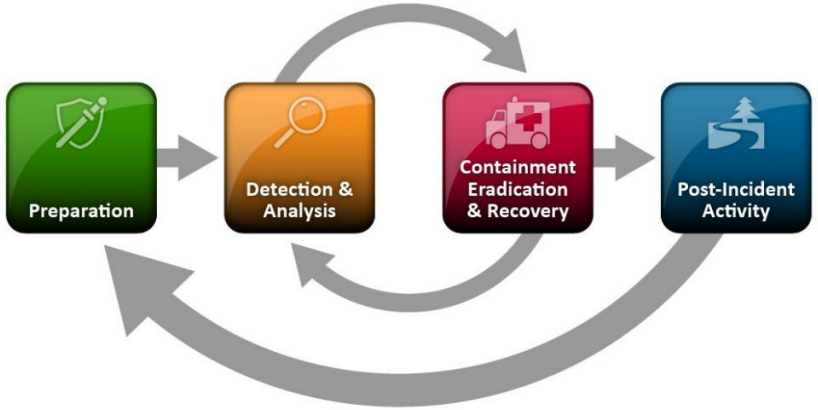
Incident Response Capability



Containment, Eradication & Recovery

- Choose a Containment Strategy
- Evidence Gathering & Handling
- Identify the Attacking Host(s)
- Eradication & Recovery

Incident Response Capability



Post-Incident Activity

- Lessons Learned
- Leverage Collected Data
- Evidence Retention
- Checklist

Incident Response Capability

Reporting

Timeliness

Communicate identified associated weaknesses

Automate when possible and if feasible

secure THINKING

Personnel awareness

Incident Response Capability

Responsibilities

CSA ISO

- Identify & assign POCs
- Collect information
- Develop, implement, maintain IR procedures
- Collect & disseminate information downstream
- POC for state IR assistance

Local Agencies

- Report
- Implement procedures
- Attend training
- Collect & maintain evidence
- Remain vigilant

Incident Response Capability

Resources

- Nationwide agencies:
  - Alerts / Advisories
  - Threat Analysis Reports
  - Incident assistance
- CSA ISO / FBI CJIS ISO / FBI FO

MS-ISAC

Multi State Information Sharing and Analysis Center

- The mission of the MS- ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

CISA

Cybersecurity and Infrastructure Security Agency

- The CISA leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

US-CERT

United States Computer Emergency Readiness Team

- The US-CERT is responsible for analyzing and reducing cyber threats, vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

Incident Response Capability

Sources

MS-ISAC

- Multi State Information Sharing and Analysis Center (MS-ISAC)
- Center for Internet Security
- Open to all U.S. SLTT government entities
- No cost (DHS funded)
- Cyber incident assistance: Cyber Incident Response Team (CIRT)
- https://www.cisecurity.org/ms-isac

Example of Services Included with Membership:

- 24/7 Security Operation Center
- Incident Response Services
- Advisories and Notifications
- Cyber Alert Map
- Weekly Top Malicious Domains/IP Report
- Monthly Members-only Webcasts
- Awareness and Education Materials

Incident Response Capability

Sources

CISA

- Cybersecurity & Infrastructure Security Agency (CISA)
- Open to all U.S. SLTT government entities
- Regionalized: Kansas City
- Cyber incident assistance: Computer Emergency Readiness Team (CERT)
- https://www.cisa.gov/

Example of Services Included with Membership:

- Cybersecurity
- Infrastructure Security
- Emergency Communications
- National Risk Management
- https://www.cisa.gov/publication/cisa-services-catalog

Incident Response Capability

Sources

US-CERT

- United States Computer Emergency Readiness Team (US-CERT)
- Open to all U.S. SLTT government entities
- No cost (DHS funded)
- Cyber incident assistance: Cyber Incident Response Team (CIRT)
- https://www.cisa.gov/uscert/

Example of Services:

- Advanced network and digital media analysis expertise
- Scoped on malicious activity targeting the networks within the United States and abroad
- Resources for SLTT:
  - https://www.cisa.gov/uscert/resources/sltt

Modernized IR Controls

Modernized IR Controls

- Fifteen (15) controls
  - 28 requirements
  - 13 new
- Total current CJISSECPOL Section 5.3 replacement

- Review policy/procedures annually/after incidents
- Review/update training content / IR training on breach
- IR testing / org elements with related plans
- Incident handling
- Reporting, supply chain notification
- Incident response assistance, automated methods
- Update plan based on org changes or problems during implementation/execution/testing / PII breaches

FBI CJIS ISO Resources

iso@fbi.gov

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

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

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	[redacted]		"	*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	[redacted]	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

Mapping to NIST 800-53 r5

- Auxiliary document to the CJIS Security Policy
- Maps Policy (v5.9) sections to related NIST SP800-53r5 controls
  - Moderate impact level controls plus some related controls
- Technical assessments for federal systems require the use of NIST controls for compliance evaluation (e.g., FISMA, FedRAMP)
- Not all Policy requirements map to NIST controls
  - Policy requirements originate from 28 CFR
  - Policy requirements unique to CJI

iso@fbi.gov

CJIS Security Policy Resource Center

- Publicly Available
- Features:
  - Search and download the CJIS Security Policy
  - Download the CJIS Security Policy Requirements Companion Document
  - Use Cases (Advanced Authentication and others to follow)
  - Submit a Question (question forwarded to CJIS ISO Program)
  - Links of importance

iso@fbi.gov

CJIS Security Policy Resource Center

SERVICES

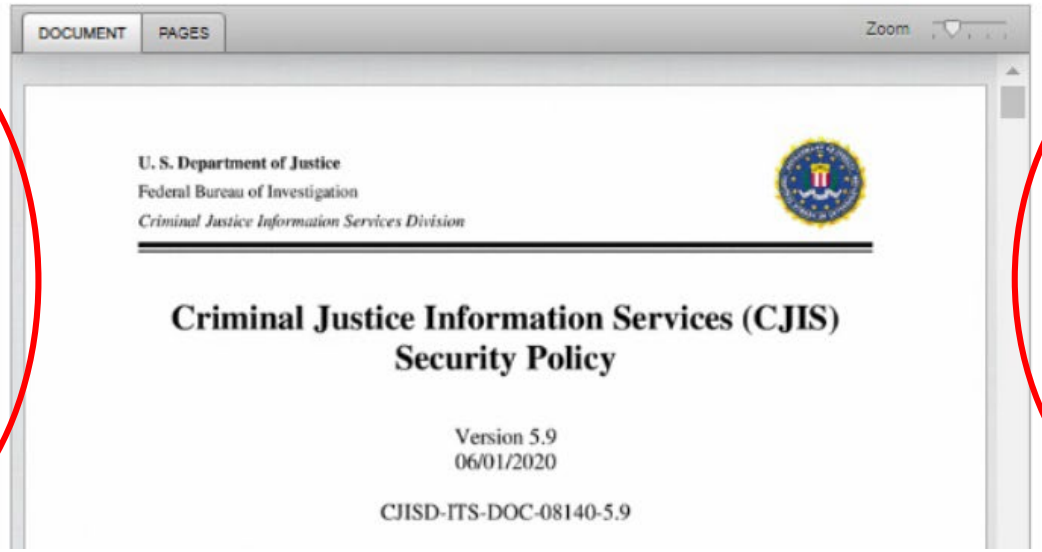
Criminal Justice Information Services (CJIS) | CIRG | Laboratory Services | Training Academy | Operational Technology | Information Management

Biometrics | Identity History | LEEP | N-DEx | NICS | NCIC | Advisory Process | Compact Council | More

CJIS Security Policy Resource Center

Requirements Companion Document | Security Control Mapping of CJIS Security Policy | 2019 ISO Symposium Presentations | Use Cases | Mobile Appendix | Submit a Question | Links of Importance

Download CJIS Security Policy (PDF)

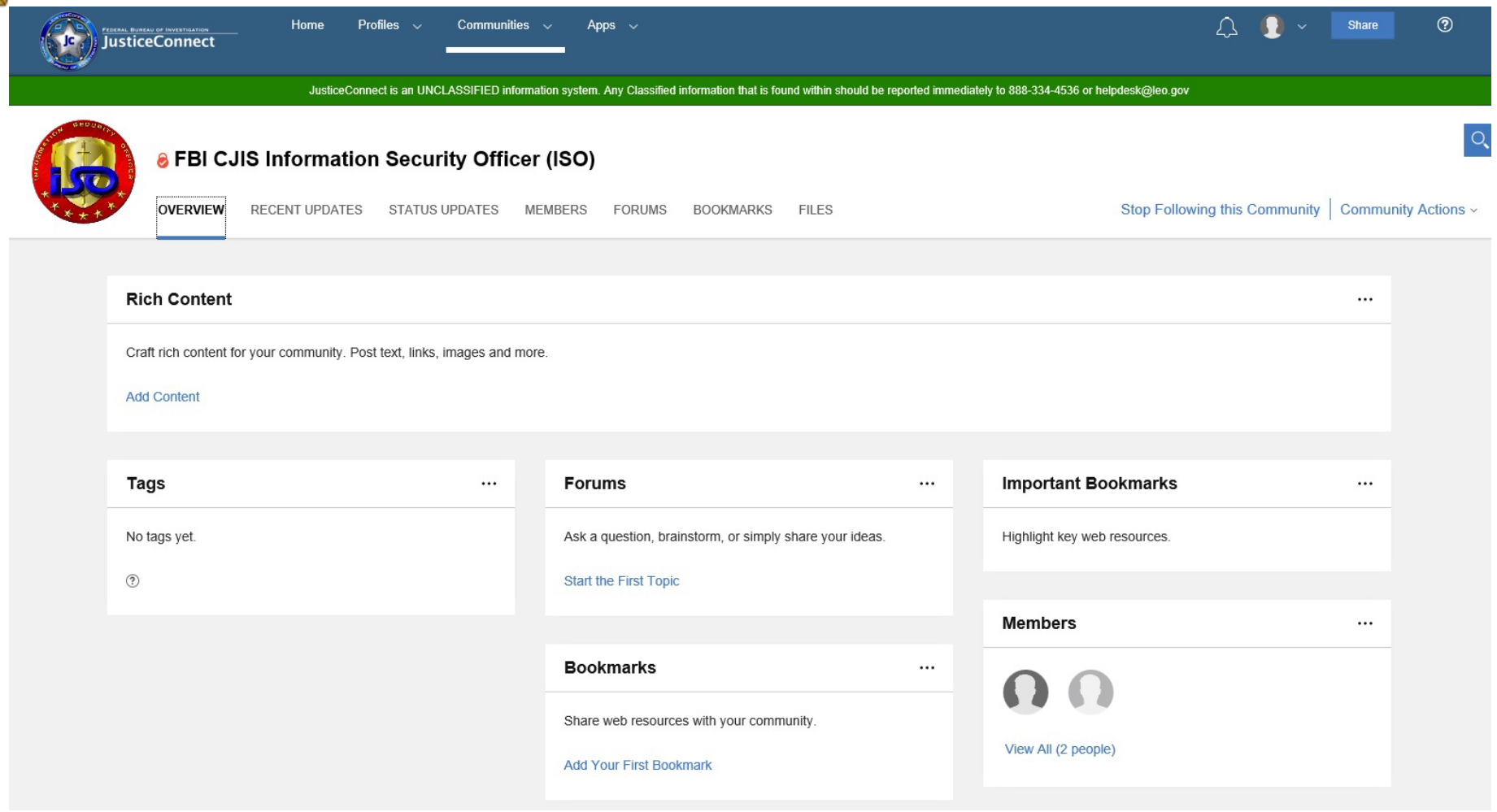


FAQs

No FAQs for this section

CJIS Security Policy Resource Center

CJIS ISO LEEP
JusticeConnect CoI



CJIS ISO Contact Information

Chris Weatherly **FBI CJIS ISO**	**(304) 625 – 3660** **jcweatherly@fbi.gov**
Jeff Campbell **FBI CJIS Deputy ISO**	**(304) 625 – 4961** **jbcampbell@fbi.gov**
Holden Cross **Sr. Technical Analyst**	**(304) 625 – 4277** **hdcross@fbi.gov**

iso@fbi.gov