Cyber Incident Resource Guide for Governors

The Cyber Incident Resource Guide for Governors provides information for governors and their staff on how to request federal support during or following a cyber incident.[1] This includes information to help states respond effectively to a cyber incident and guidance to support recovery efforts. For states with mature cyber programs, this Guide can validate and integrate with existing plans. The scope of this document includes cyber incident response; however, appropriate cyber risk management practices can lessen the likelihood or impact of an incident. Refer to Appendix B – Cyber Resilience Resources for information on cyber resilience and related cyber risk management resources. **This Guide does not replace a state's cyber incident response plan**.

CYBER INCIDENT RESPONSE

Victims of cyber incidents can report to the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), or the United States Secret Service (USSS). These agencies share information with interagency partners; therefore, a state only needs to report an incident once to notify all the other federal agencies who have a role in incident response. Federal agencies collaborate to help states and other affected entities understand the cyber incident, link related incidents, and share information to rapidly respond to and mitigate the incident in a manner that protects privacy and civil liberties. In accordance with Presidential Policy Directive 41 (PPD-41)[i], upon receiving a report of a cyber incident, the Federal Government focuses its efforts on two activities: Asset Response (Lead: DHS, through CISA) and Threat Response (Lead: DOJ, through FBI). A third line of effort is Intelligence Support (Lead: Office of the Director of National Intelligence (ODNI)). These federal activities integrate with and support the state response (Figure 1).

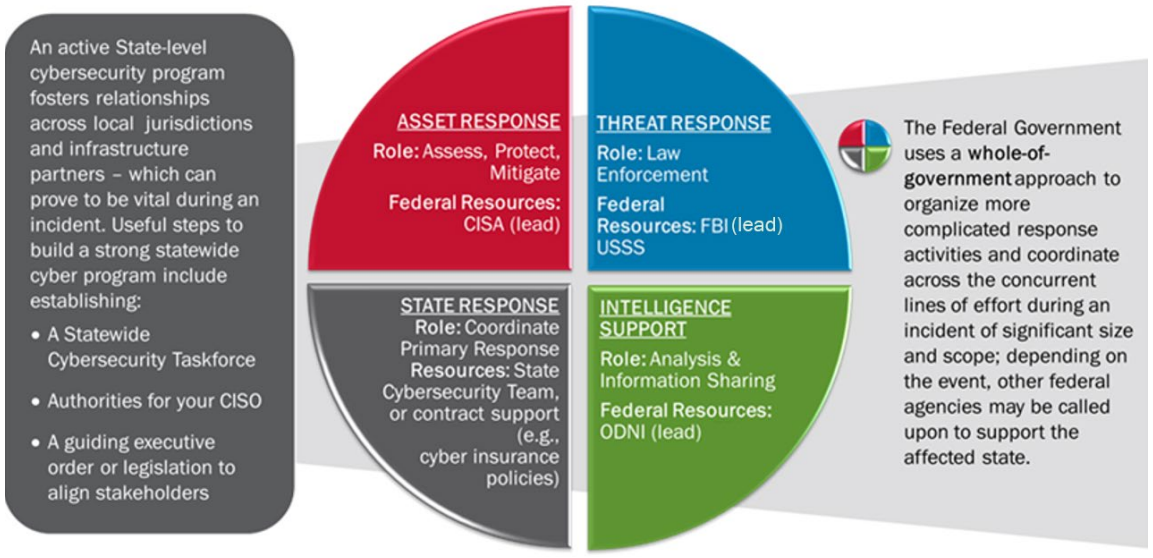


Figure 1: Cyber Incident Response Concurrent Lines of Effort

[1] A cyber incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of digital information or an information system and that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (Source: https://csrc.nist.gov/glossary/term/incident)

The Federal Government delineates cyber incident response roles as outlined in the table below.

Asset Response *ASSESS, PROTECT, MITIGATE* ♦ Lead Agency: CISA	♦ Provides technical assistance to protect assets and mitigate vulnerabilities in the face of malicious cyber activity ♦ Reduces the impact to systems and/or data ♦ Strengthens, recovers, and restores services ♦ Identifies other entities at risk ♦ Assesses potential risk to the sector or region ♦ Facilitates operational information sharing and coordination ♦ Provides guidance on how to best use federal resources and capabilities
Threat Response *LAW ENFORCEMENT* Lead Agency: FBI	♦ Attributes, pursues, and disrupts malicious cyber actors and malicious cyber activity ♦ Conducts criminal investigations and other actions to counter the malicious cyber activity
Intelligence Support *ANALYSIS AND INFORMATION SHARING* Lead Agency: ODNI	♦ Builds situational threat awareness ♦ Shares related intelligence with asset and threat response organizations ♦ Integrates analysis of threat trends and events ♦ Identifies knowledge gaps ♦ Evaluates the ability to degrade or mitigate adversary threat capabilities

REPORTING A CYBER INCIDENT

Cyber incidents resulting in significant damage are of particular concern to the Federal Government. States are encouraged to report all cyber incidents that may:

- Result in a significant loss of data, system availability, or control of systems;
- Impact a large number of victims;
- Indicate unauthorized access to, or malicious software present on, critical IT systems;
- Affect critical infrastructure or core government functions; or
- Impact national security, economic security, or public health and safety.[ii]

States can report cyber incidents at various stages, including before complete information is available. Gathering as much information as possible will help expedite assistance to an affected entity. Reporting an incident as soon as practicable may assist affected entity efforts to contain the incident and avoid additional impacts.

After reporting an incident to CISA, FBI, or USSS, based on incident severity, the Federal Government gathers additional information to evaluate the incident and communicate with you regarding available assistance resources.

Contact information to report cyber incidents to the Federal Government is listed in Appendix C.

INCIDENT SCORING AND CISA ASSET RESPONSE SUPPORT

CISA created the National Cyber Incident Scoring System (NCISS) based on the Cyber Incident Severity Schema outlined in PPD-41. The NCISS provides a repeatable and consistent risk score. This risk score is used to help determine the prioritization of limited asset response resources and the necessary level of support. An incident is assigned a rating of baseline, low, medium, high, severe, or emergency.[iii]

Based on a state's voluntary incident report to CISA, associated scoring, and available resources, CISA determines which type of support to provide (See Appendix C for specific capabilities):

- Remote assistance (the most frequent type of support provided): Services are provided via video calls, phone calls and email;
- Advisory deployment: Only Subject Matter Expert support is provided;
- Remote deployment: No teams are deployed. Personnel are deployed only to configure remote operations equipment; and
- On-site deployment: Equipment and personnel are deployed onsite.

The vast majority of incidents reported to CISA are scored as baseline or low (i.e., they are unlikely to impact public health or safety, national security, or other threats to the nation).

STATE/FEDERAL COORDINATION

The state maintains primary responsibility for managing the effects of cyber incidents on its operations, constituents, and workforce. An affected state engages in a variety of efforts to manage the impact of a cyber incident, which may include maintaining business or operational continuity; addressing adverse financial impacts; protecting privacy; complying with legal and regulatory requirements (including disclosure and notification); engaging in communications with employees or other affected individuals; and dealing with external affairs (e.g., media and congressional inquiries).

State cybersecurity officials may reference CISA's Incident Response and Vulnerability Management Playbook for detailed guidance on creating and executing a cyber incident response plan.

Two changes in version 3 of FEMA's Comprehensive Preparedness Guide (CPG) 101 add flexibility to cyber considerations. CPG-101 now has a Cyber Incident Annex in its templates. According to CPG-101, a Cyber Incident Annex to an Emergency Operations Plan (EOP):

> "…identifies and describes the jurisdiction's specific concerns, capabilities, training, agencies and resources to respond to an intentional event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity or availability of computers; information or communications systems or networks; physical or virtual infrastructure controlled by computers or information systems; or information resident on those systems. Note: Cyber incidents can also result from accidents and unintentional system failures."

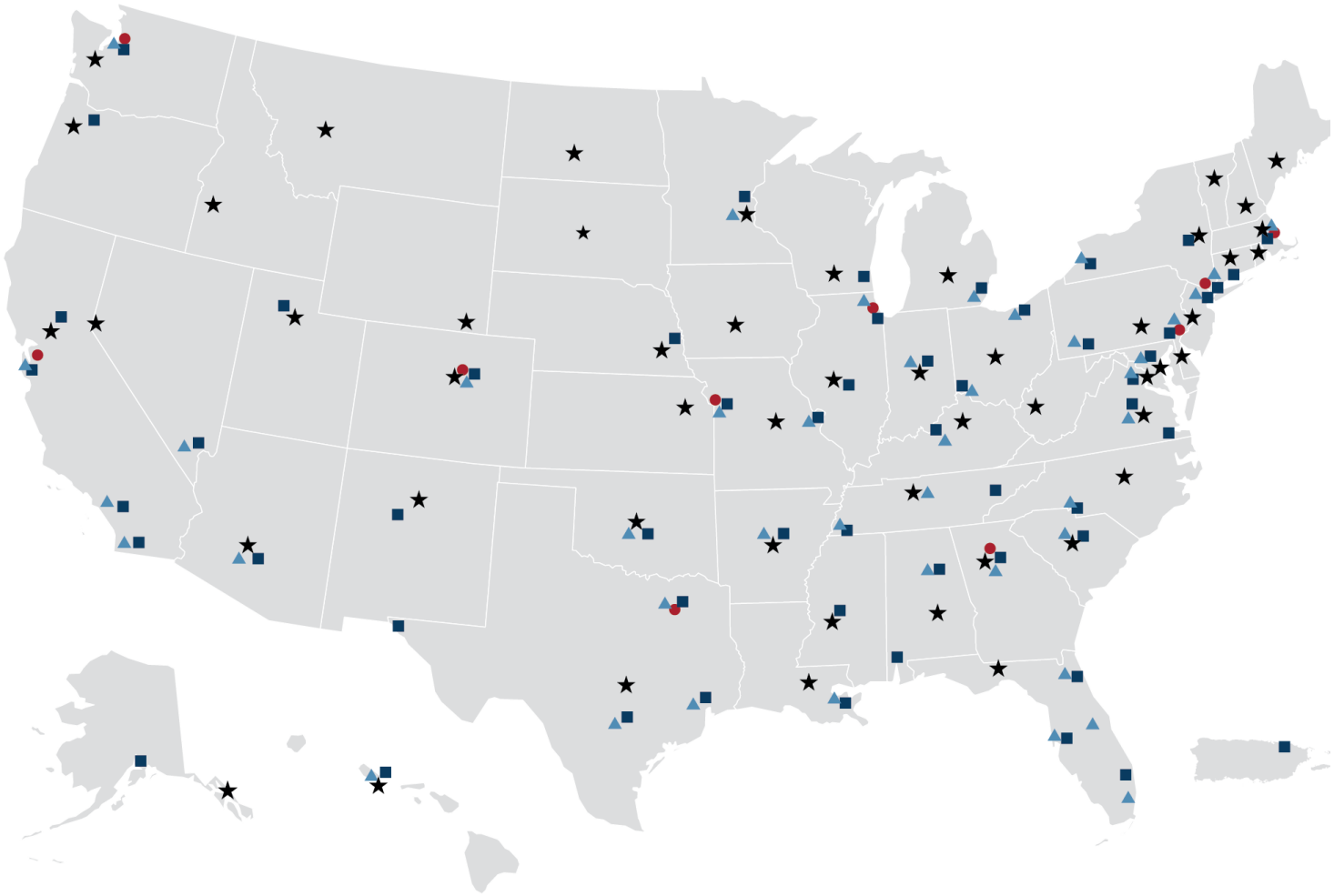
In addition, EOPs are no longer required to align annexes to Emergency Support Functions (ESFs). Whether or not state EOPs follow an ESF structure, the Cyber Incident Annex provides guidance for a state's emergency management organization. State-level EOPs that use an ESF structure can embed cyber response activities into applicable ESFs for use by emergency management personnel, for example:

- In Ohio's Emergency Operations Plan, their cyber response plan is found in ESF 2 – Communications and Information Technology as "Tab B - Cyber Incident Response Plan;"[iv] and
- California's Emergency Plan provides a standalone ESF titled "18 CA-ESF Cybersecurity Annex."[v]

Some state cyber incident plans identify federal-level response partners. For example, consistent with PPD-41, South Carolina's Emergency Operations Plan specifically identifies CISA and the FBI for federal-level asset response and threat response support roles, respectively.[vi]

It is important to note that CPG-101 provides guidance to emergency management organizations on how to develop a Comprehensive Emergency Management Plan (CEMP) to document all-hazard capabilities. A state's chief information officer (CIO) or chief information security officer (CISO) may have a stand-alone cyber incident response plan. Regardless of whether a state embeds cyber response into an existing CEMP or establishes a separate cyber incident response plan, each state should clearly identify where they integrate considerations for coordinating with the Federal Government on cyber incident response.

APPENDIX A – CISA REGIONAL OFFICES, FBI FIELD OFFICES, SECRET SERVICE FIELD OFFICES



KEY: ★ = State Capitals ▲ = US Secret Service Field Offices ■ = FBI Field Offices ● = CISA Regional Offices

All states have cybersecurity coordinators on site or in various stages of processing before reporting for duty.

KEY TO MAP OF FIELD OFFICES

State	City	CISA Regional Office	FBI Field Office	USSS Field Office
Alabama	Birmingham		■	▲
	Mobile		■	
Alaska	Anchorage		■	
Arizona	Phoenix		■	▲
Arkansas	Little Rock		■	▲
California	Los Angeles		■	▲
	Oakland	■ (Region 9)		
	San Diego		■	▲
	San Francisco		■	▲
	Roseville		■	
Colorado	Denver	■ (Region 8)	■ (Colorado and Wyoming)	▲ (Colorado, Wyoming, Utah, southern Idaho)
Connecticut	New Haven		■	
District of Colombia	Washington	■ (HQ)	■ (HQ)	▲ (HQ)
Florida	Jacksonville		■	▲
	Miami			▲
	Miramar		■	
	Orlando			▲
	Tampa		■	▲
Georgia	Atlanta	■ (Region 4)	■	▲
Hawaii	Honolulu			▲
	Kapolei		■	
Illinois	Chicago	■ (Region 5)	■	▲
	Springfield		■	
Indiana	Indianapolis		■	▲
Kentucky	Louisville		■	▲
Louisiana	New Orleans		■	▲
Maryland	Baltimore		■ (Maryland and Delaware)	▲
Massachusetts	Boston	■ (Region 1)	■ (Maine, Massachusetts, New Hampshire, and Rhode Island)	▲
	Chelsea		■	
Michigan	Detroit		■	▲
Minnesota	Brooklyn Center		■	
	Minneapolis		■ (Minnesota, North Dakota, and South Dakota)	▲

CISA REGIONAL PERSONNEL

CISA has ten regions, aligned to the FEMA regions. Through offices[vii] in each region, regional personnel manage mission execution through steady state and incident operations and analyze risks to critical infrastructure. Each Regional Director leads a cadre of security professionals located throughout the region.

Each CISA Region has local and regional Cybersecurity Advisors (CSAs), Cybersecurity State Coordinators (CSCs), Protective Security Advisors (PSAs), Emergency Communications Coordinators, and other CISA personnel. These field personnel advise and assist in training and exercising best practices to help achieve robust resilience.

- **CSAs** prepare and protect a state from cybersecurity threats by helping partners enhance cybersecurity preparedness, risk mitigation, and incident response capabilities. They engage stakeholders through partnership and direct assistance activities, including policy-based cybersecurity assessments.
- **CSCs** are appointed to serve in each state. CSCs serve as the federal cybersecurity risk advisors; support cybersecurity preparation, response, and remediation efforts; facilitate the sharing of cyber threat information; and help SLTT governments develop cybersecurity plans.
- **PSAs** are trained critical infrastructure protection and vulnerability mitigation subject matter experts who facilitate local field activities in coordination with other DHS offices. They also advise and assist state, local, and private sector officials and critical infrastructure facility owners and operators.
- **Emergency Communications Coordinators** support emergency communications interoperability by offering training, tools, workshops, and regional support. CISA assists emergency preparedness communities in establishing seamless and secure communications, supporting public safety and national security.

BUILDING CYBER RESILIENCE THROUGH THE JOINT CYBER DEFENSE COLLABORATIVE

As we look to the future of building cyber resilience across the nation, CISA has established a new collaborative to strengthen cybersecurity collaboration across the Federal Government, private sector critical infrastructure owners and operators, and SLTT governments. The JCDC is a forum to develop deliberate and rapid and reactive plans for whole-of-nation cyber defense operations.

As critical JCDC partners, SLTT entities will have the opportunity to participate in planning efforts to jointly defend critical systems and our country's national critical functions against malicious cyber activity. CISA encourages cross-functional, whole of entity participation in JCDC. Depending on state preferences and organizational structure, this may include representation from the Governor's Office, state CIO or CISO's Office, Homeland Security, Emergency Management, Fusion Center, State Police, or Elections.

For more information on JCDC, see www.cisa.gov/jcdc or contact CyberLiaison_SLTT@cisa.dhs.gov.

ADDITIONAL CYBER RESILIENCE RESOURCES

Table 2 lists resources for additional information on important topics such as assessments, cyber planning, and cyber grants.

Table 2: Steady State Services

Support Mechanism and Website	Description
CISA Cyber Essentials	A **guide for leaders** of small businesses and small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity best practices.
CISA Cyber Resource Hub	A range of **cybersecurity assessments** that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust and resilient cyber framework.
CISA Incident Response Training	No-cost cyber **incident response training** for government employees and contractors across federal and SLTT governments.
CISA Ransomware Guide	A **guide** aimed at being a one-stop resource with best practices and ways to prevent, protect and/or respond to a ransomware attack. Includes a ransomware response checklist.
CISA SAFECOM	A **series of documents** that includes resources about the National Emergency Communications Plan, education and outreach programs, and the specific issues and barriers that affect interoperability of communications.
Federal Government Cybersecurity Incident and Vulnerability Response Playbooks	A standard set of **operational procedures** to be used in planning and conducting cybersecurity vulnerability and incident response activities for federal civilian agency information systems. Also applicable for SLTT government use.
Multi-State Information Sharing and Analysis Center	Funded by CISA as the focal point for **cyber threat prevention, protection, response, and recovery** for the Nation's SLTT governments.
Nationwide Cybersecurity Review	A **no-cost, anonymous, annual self-assessment conducted by the MS-ISAC on CISA's behalf** to measure gaps and capabilities of SLTT governments' cybersecurity programs. Based on the National Institute of Standards and Technology Cybersecurity Framework.
National Institute of Standards and Technology Cybersecurity Framework	A **framework of standards, guidelines, and practices** to promote the protection of critical infrastructure. The framework's prioritized, flexible, repeatable, and cost-effective approach helps owners and operators of critical infrastructure manage cybersecurity-related risk.

APPENDIX C – FEDERAL CYBER INCIDENT RESPONSE CONTACTS

Federal Asset Response Contacts	Federal Threat Response Contacts
Federal **asset response** includes: • Providing technical assistance to affected entities, upon request, to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents while identifying other entities that may be at risk; • Assessing potential risks to the sector or region; • Facilitating information sharing and operational coordination; and • Providing guidance on how to best use federal resources and capabilities.	Federal **threat response** includes law enforcement and national security investigative activity, including: • Collecting evidence and intelligence; • Developing attribution; • Linking related incidents; • Identifying additional affected entities; • Identifying threat pursuit and disruption opportunities; • Developing and executing action to mitigate the immediate threat; and • Facilitating information sharing and operational coordination with asset response.
What You Can Expect: • Specific guidance to help evaluate and remediate cyber incidents; • Remote assistance to identify the extent of the compromise and recommendations for appropriate containment and mitigation strategies; and • Analysis of phishing emails, storage media, logs, and malware (full-disk forensics on an as-needed basis).	**What You Can Expect:** • Assistance in conducting a criminal investigation, which may involve collecting incident artifacts, to include system images and malware samples.
CISA Central: • https://us-cert.cisa.gov/report • Central@cisa.gov • (888) 282-0870 **CISA Cybersecurity Advisor** • https://www.cisa.gov/cisa-regions • [Enter your local CISA CSA's phone and email] **CISA Cybersecurity State Coordinator** • [Enter your local CISA CSC's phone and email]	**FBI Field Office:** • https://www.fbi.gov/contact-us/field-offices/ • [Enter your local FBI field office POC phone and email]
MS-ISAC Coordination[viii] An expertly trained Computer Incident Response Team (assists SLTT organizations, including by providing the following free services: emergency conference calls, forensic analysis, log analysis, mitigation recommendations, and reverse engineering.	**U.S. Secret Service Cyber Fraud Task Force(s)**[ix] **Coordination:** The Special Agent in Charge from the nearest field office assesses the situation, then activates other assets as needed. This may include cyber forensics teams and/or network intrusion responders. Any dignitary protection mission in the area takes precedence and may delay deployment.
• soc@msisac.org • (866) 787-4722	**USSS Field Office:** • https://www.secretservice.gov/contact/field-offices • [Enter your local USSS field office POC phone and email]

APPENDIX D – ENDNOTES

[i] Presidential Policy DirectivePPD-41 – United States Cyber Incident Coordination

[ii] Cyber Incident Reporting United Message.pdf (dhs.gov)

[iii] CISA National Cyber Incident Scoring System

[iv] https://ema.ohio.gov/EOP_Overview.aspx;

[v] https://www.caloes.ca.gov/cal-oes-divisions/planning-preparedness/state-of-california-emergency-plan-emergency-support-functions

[vi] https://scemd.org/media/1367/appendix-16-sc-cyber-incident-consequence-managment-plan.pdf

[vii] https://www.cisa.gov/cisa-regions

[viii] https://www.cisecurity.org/isac/report-an-incident/

[ix] https://www.secretservice.gov/investigation/cyber