State Cyber Disruption Response Plans

ISSUE BRIEF | JULY 2019

General Overview

Governors must now be prepared to respond to the growing threat of cyberattacks. States and territories count on experienced teams of public safety and emergency management (EM) professionals to prepare for, respond to and recover from natural and human-made disasters. With the integration of information technology (IT) into critical services, state and territorial officials must now expand their focus to consider the consequences of cyberattacks that have physical impacts and threaten public safety. Malicious actors have already shown a keen interest in targeting state and local assets. In 2016, a ransomware attack disrupted operations at the San Francisco Municipal Transportation Agency.[1] The following year, malware shuttered the largest terminal at the Port of Los Angeles.[2] In 2018, former Colorado Gov. John Hickenlooper declared a state of emergency — the first of its kind — after a ransomware attack infected 150 servers and 2,000 computers operated by the Colorado Department of Transportation (DOT).[3]

This issue brief examines state ***cyber disruption response plans*** that governors are developing and testing in preparation for cyberattacks that demand coordination across state agencies. These plans detail the agencies that must respond to an incident, their roles and responsibilities (R&Rs), and how they will coordinate resources. This issue brief also examines how these plans align with the U.S. Department of Homeland Security (DHS) National Cyber Incident Response Plan (NCIRP), which establishes protocols to guide any federal and state response to a "significant cyber incident."* It concludes with recommendations for state leaders who are creating or revising their own response plans.

* The NCIRP does not force or provide funds to states for following these protocols.

State Cybersecurity and Response Planning

As state and territorial governments digitized, they implemented new protections for electronic data that they collected, transmitted or stored. Chief information officers (CIOs) and chief information security officers (CISOs) created ***incident response plans*** to detail how they would protect, respond to and recover from ***cyber incidents*** — that is, cyberattacks that compromise the confidentiality, integrity or availability of this data.[4] Because these plans typically address potential incidents that affect state IT infrastructure, their development and execution generally fall under the purview of the state CIO, who is empowered to perform most of the necessary functions. Although these incidents typically affect IT infrastructure only, they can have tremendous consequences. In 2012, hackers infiltrated **South Carolina**'s Department of Revenue and stole nearly 4 million tax records and roughly 400,000 credit card numbers, costing the state at least $18 million.[5]

States are now developing ***disruption response plans*** to prepare for, respond to and recover from a ***significant cyber incident*** — cyberattacks that "pose demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of [the public]."[6] These plans differ from incident response plans because they require multiple agencies to coordinate activities and implement traditional EM and homeland security (HS) operations. According to publicly available information, the United States has not yet experienced a significant cyber incident. Malicious actors, however, have not shied away from cyberoperations that pose serious physical consequences. Malicious actors' meddling with Ukraine's electric grid and the attempted explosion targeting a Saudi Arabian petrochemical plant exemplifies the potential impact of a significant cyber incident in the United States.[7] Like a Category 5 hurricane, states realize that they have a role in mitigating the impact of such a scenario and are solidifying those R&Rs in cyber disruption response plans.

State Cyber Disruption Response Plans

The National Governors Association (NGA) Center for Best Practices has identified 15 states with publicly available cyber disruption response plans.[†] Among these plans, four were drafted after the release of the NCIRP.[‡] Older plans integrate federal policies and guidelines, such as the National Institute for Standards and Technology Cybersecurity Framework and the National Cyberspace Security Response System described in the National Strategy to Secure Cyberspace or a draft of the NCIRP.

Among the 15 states reviewed, nine wrote their plans as an annex to the state emergency operations plan (EOP),[§] two wrote their plans as an appendix to the state EOP, two wrote their plans as stand-alone documents,[8] one integrated its plan throughout its EOP and one wrote its plan as a separate Emergency Support Function (ESF). (See Table 2 in the Appendix.) (States have created cyber disruption response plans as a separate ESF (e.g., **Massachusetts**) or as a stand-alone document to have the benefit of elevating the importance of cybersecurity within their EOP.[**]) Every plan reviewed emphasizes a whole-of-state approach, recognizing the all-encompassing impact a significant cyber incident can have.

In determining when to activate their plans and how to execute a response, the states rely on cyberthreat schemas. Seven types of threat schemas were identified within the 15 plans, with five states not specifically detailing a schema but identifying when the plan would be activated:

- Two states use a five-level threat schema. **Connecticut**'s threat schema, for example, ranges from "low" to "emergency" and provides a definition of the level, the escalation criteria, de-escalation criteria, potential impact and the communications procedure.
- One state uses a four-level threat schema, ranging from "low" to "emergency," and identifies six incident categories with corresponding frequency of occurrence and areas of concern, including system fault, accident, disaster, computer crimes, cyberterrorism and acts of war.
- Two states use a three-level threat schema. For example. **Maine** has descriptions for what constitutes "minor," "major" and "disaster."
- One state uses a two-level threat schema.
- Three states detail specific R&Rs, activities, escalation and communication procedures during each threat level.
- One state uses an escalation and notification matrix but does not detail a threat schema.
- One state uses a risk assessment methodology. (See Table 3 in the Appendix.)

[†]Although only 15 states could be publicly identified, NGA is aware of state efforts to create cyber disruption response plans and states that have privately held documents.

[‡] Arizona, Connecticut, South Carolina and Wisconsin.

[§] An EOP is a comprehensive document that every state maintains to detail how it would respond to natural and human-made disasters.

[**] The motives behind each approach are a topic for further investigation.

NATIONAL GOVERNORS ASSOCIATION
444 N. Capitol Street NW, Suite 267 | Washington, DC 20001 | 202.624.5300 | NGA.org

Even where states select the same threat schema, they may categorize the severity of a cyber incident differently. Some plans provide discretion to a senior state leader to determine the threat level, as in **Wisconsin**.

Once the plan is activated, these states invoke preplanned leadership structures to oversee response efforts, which varies by state. Six states identified a joint leadership structure with their IT and HS/EM agencies, six states identified their IT agency as their lead agency and three states identified their HS/EM agency as the lead. (See Table 4 in the Appendix.) In state plans where one agency serves as the lead, IT and HS/EM were identified as supporting agencies with significant R&Rs.

However, each state emphasized the whole-of-state approach when identifying supporting agencies, with several either activating other ESFs[††] or simply stating "other agencies as needed" when detailing R&Rs. (See Table 5 in the Appendix.) The plans varied in their level of detail in describing each agency's R&Rs, but the plans primarily identified the following functions:[‡‡]

- **State IT agencies:** Lead, co-lead or support response efforts and perform technical response and recovery activities.
- **EM/HS:** Lead, co-lead or support response efforts and perform traditional EM and HS functions.
- **Law enforcement agencies (LEAs).** Conduct investigations.
- **Fusion centers.** Perform interstate and intrastate information-sharing functions.
- **National Guard units.** Use their cyber assets for cybersecurity or EM functions; for example, National Guard units could perform tabletop exercises or conduct penetration testing with partners. (See Table 6 in the Appendix.)

Finally, in the event of a significant cyber incident, state plans establish a unified coordinating group (UCG) to coordinate R&Rs. The UCG is a communication and coordinating structure based on the National Incident Management System's (NIMS) Incident Command System (ICS).[9] Notably, three states would establish a specific cyber UCG, similar to the federal government (see below), and eight states would deploy technical experts from the lead and supporting agencies' cybersecurity response team (CRTs) to help the affected entity contain, eradicate and repair its systems. (See Table 7 in the Appendix.)

[††] Typically, an EOP has 16 ESFs that identify the state agencies that would respond to an incident. Several cyber disruption response plans note that other or all ESFs could be activated during a significant cyber incident.

[‡‡] Each plan detailed the R&Rs for federal entities, but these R&Rs are not included in the appendix because they are identical for each state. Please see the NCIRP for these R&Rs.

The National Cyber Incident Response Plan

Like other significant human-made and natural disasters, states would partner with the federal government to respond to and recover from significant cyber incidents. The Obama administration published two documents that detail the federal government's response to a significant cyber incident: Presidential Policy Directive 41 (PPD-41) and the NCIRP. In brief, PPD-41 details the R&Rs of the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence and DHS and describes a five-level cyber incident severity schema.[10] (See Figure 1.) DHS identifies the severity of a an incident in part by "consult[ing] with critical sector leadership and private sector owners and operators directly and/or through various organizations (e.g., Information Security and Analysis Centers, Sector Coordinating Councils)."[11]

Figure 1: Cyber Incident Severity Schema

Description	Disaster Level	Cyber Incident Severity	Description	Observed Actions
Due to its severity, size, location, actual or potential impact on public health, welfare, and infrastructure it requires an extreme amount of federal assistance for response and recovery efforts for which the capabilities to support do not exist at any level of government.	Level 1	Level 5 *Emergency*	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.	Effect
Requires elevated coordination among federal and SLTT governments due to moderate levels and breadth of damage. Significant involvement of FEMA and other federal agencies.	Level 2	Level 4 *Severe*	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Presence
		Level 3 *High*	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
Requires coordination among federal and SLTT governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.	Level 3	Level 2 *Medium*	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Engagement
		Level 1 *Low*	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
No event or incident anticipated. This includes routine watch and warning activities.	Level 4	Level 0	Unsubstantiated or inconsequential event.	Steady State

Source: Presidential Policy Directive 41, United States Cyber Incident Coordination.

Once DHS scores an incident, key stakeholders — federal; private; state, local, tribal and territorial (SLTT); and affected entities — undertake four concurrent "lines of effort": threat response, asset response, intelligence support and affected entities response. [12] (See Table 1 for an overview of activities within each line of effort.) The NCIRP also details 14 core capabilities for fulfilling each response activity, such as access control and identification verification, forensics and attribution, and operational communications.

Table 1: NCIRP Lines of Effort[13]

Threat response	Asset response	Intelligence support	Affected entity response
• Investigative, forensic, analytical and mitigation activities. • Interdiction of a threat actor. • Providing attribution.	• Furnishing technical support to affected entities. • Mitigating vulnerabilities, identifying additional at-risk entities. • Assessing affected entities' risk to the same or similar vulnerabilities.	• Activities to better understand the cyber incident and existing targeted diplomatic, economic or military capabilities to respond. • Sharing threat and mitigation information with other potentially affected entities or responders.	• Maintaining business or operational continuity. • Mitigating potential health and safety impacts. • Addressing adverse financial impacts. • Protecting privacy • Managing liability risk; complying with legal and regulatory requirements (including disclosure and notification). • Engaging in communications with employees or other affected individuals. • Managing external affairs.

The NCIRP details general and specific recommendations for state entities within these four lines of effort. For threat response and intelligence support, for example, the NCIRP advises that states' primary responsibility is to share information with federal, public and private entities and to "act as the conduit between the affected entity and the federal government."[14]

Regarding asset response, the NCIRP is more specific. It says:

- Each state is responsible for developing a plan that describes its role in asset response for entities within the state. This state plan should be consistent with the NCIRP and serve as a cyber annex to its respective state EM plan.[15]
- To facilitate coordination during a significant cyber incident response operation, each key executive should predesignate a primary individual to serve as senior official to represent its government. Until amended by each key executive, DHS' National Cybersecurity and Communications Integration Center (NCCIC) uses the state homeland security advisor (HSA) as its primary point of contact.[16]
- Governance is vital and an enabling factor in states' cyber asset response role. This role includes the supporting legal framework, policies, plans and procedures that codify the state CISO's authority and responsibilities.[17]
- At the direction of the state's governor and the adjutant general (TAG), the National Guard can perform state missions, including supporting civil authorities' response to a significant cyber incident (e.g., reimaging; identifying and defeating the malware).[18]
- SLTT community leaders and points of contact may be asked to provide advice, support and assistance to federal departments and agencies on preparedness and response activities related to SLTT priorities (e.g., HSAs, CIOs, CISOs).[19]
- SLTT entities should be prepared to request additional resources from the federal government — for instance, under the Stafford Act — in the event of a cyber incident that exceeds their government's capabilities.[20]

Finally, akin to state response plans, the federal government would establish a cyber UCG to coordinate these efforts and integrate external partners' activities.[21] Specifically, states could be asked to "participate when they own or operate critical infrastructure (CI) that is or may be affected by a significant cyber incident."[22,§§] If the incident is affecting private infrastructure, the "Cyber UCG will use existing collaboration and information sharing mechanisms to provide regular updates to SLTT partners."[23]

§§ SLTT "participation" is not defined. Presumably, participation would include activities detailed in the "Lines of Effort."

Recommendations for Creating a State Cyber Disruption Response Plan

The 15 state plans, the NCIRP and **Colorado**'s after-action report (AAR) from its DOT cyber incident offer a useful starting point for states developing or revising their response plans. These documents provide promising practices that other states can adopt for integrating their plan with their EOP, building a severity schema, creating a leadership structure, denoting R&Rs and coordinating response efforts.

State Cyber Response Plans and the Emergency Operations Plan

- **Develop a "cyber disruption response strategy"** prior to developing a formal plan to detail the stakeholders involved in creating a response plan, the information needed to inform a plan and how frequently the plan will be exercised or updated. Prior to creating its response plan, Wisconsin created such a strategy to strengthen relations with its public and private CI and key resources (CIKR) partners, delineate R&Rs and assess risk profiles.[24] Examining partners' risks, capabilities and capacities can help states detail appropriate R&Rs, avoid duplication of effort, and identify response and recovery gaps that the state may need to fill. Finally, creating procedures to review internal and external AARs (e.g., Colorado's AAR) ensures that the plan incorporates lessons learned from prior cyber incidents.
- **Train cyber incident responders on emergency response and emergency operations center (EOC) standard operating procedures (SOPs):**[25] In Colorado, the state identified that "[h]aving ICS trained personnel on the cyber incident response team would have facilitated a common approach to incident handling and may have reduced friction points."[26]
- **Modify or create annexes for continuity of operations (COOP) plans that account for a cyber disruption event:**[27] Once again, Colorado found that its COOP plans did not anticipate challenges that would arise from a cyber incident disrupting its operations.[28]

Threat Schemas and Plan Activation

- **Use the NCCIC Cyber Incident Scoring System.** This schema determines the severity of an incident and, ultimately, when the federal government needs to become involved. If a state does not use this schema, it should at least incorporate one in the planning process so that stakeholders understand when the federal government would become involved.
- **Catalog risk assessments for public and — where possible — private CIKR partners:** It is difficult to fully implement such a catalog in practice, but risk assessments of CIKR partners can help states prioritize their limited response capabilities

for an incident that affects several entities simultaneously. **Michigan** details a formula and process for its CIKR partners to voluntarily document their risk, and partners meet regularly to discuss remediation efforts to their vulnerabilities.[29] The risk profiles help the state determine the highest priority asset to protect and recover based on those "that are most vulnerable and would have the greatest impact if disrupted."[30]

- **Attach specific protocols to each threat level:** Providing operational detail in a cyber disruption response plan could prove beneficial during an incident. Colorado identified this recommendation following the state's ransomware attack and recommended that its response plan "address escalating cyber incidents, establish triggers for response actions."[31] The state also recommended "establishing scalable command and control" to account for the potentially escalating nature of a significant cyber incident.[32] Connecticut's approach provides a definition for each threat level, escalation and de-escalation criteria, potential impact and the communications procedure. States adopting specific protocols may also want to consider how they would share information and coordinate activities with other states in the case of a regional incident.

Lead and Supporting Agencies

- **Identify the state's senior official for cybersecurity:** The NCIRP identifies the state's HSA as the default senior official for coordinating cybersecurity with DHS, unless the state specifies otherwise. Identifying this individual and appropriately integrating him or her into a leadership role could help foster information sharing and coordinate actions between the state and federal government.
- **Create an interagency leadership structure with the state's CIO or CISO, HSA, TAG and emergency manager:** States should consider creating a response-governance structure among these four disciplines; these people will have important R&Rs in the event of a significant cyber incident. A close, institutionalized partnership with these personnel could decrease assumptions, clarify priorities, and address response and recovery gap capabilities. In addition, states may need to consider how this structure mirrors or reports to the state's overall cybersecurity governance body, if one exists.[33] A cyber UCG or response team, described in Table 5 and Table 6, is one mechanism for fulfilling this goal.
- **Codify the CISO's R&Rs to foster governance, as detailed in the NCIRP:**[34] The CISO will have tremendous R&Rs during a significant cyber incident and may have to operate on state agency networks that are outside of her or his authoritative control. States should consider reviewing their statutes to ensure that the CISO has the authority to effectively carry out his or her R&Rs outside the normal authority in the event of a significant cyber incident. Formalizing these and potentially other agencies' R&Rs could be beneficial in ensuring that state agencies' roles are discussed before an incident occurs and serves as a forcing mechanism to institutionalize the response plan.

- **Include the state's public utility regulatory authority (PURA) as a supporting agency in the state's response efforts:** Connecticut identifies the PURA as a supporting agency that would assist the state's cyber response team upon request in the event of a significant cyber incident. Further, the PURA could "coordinate response to resource and assistance requests for matters pertaining to public utility operations." (See Table 5 for more information.) Other states may want to integrate their PURA into their response plans, especially if the PURA oversees cybersecurity plans of government-managed utilities.

Roles and Responsibilities

- **Include steady-state R&Rs and review the NCIRP's core capabilities:** Including preventive/steady-state R&Rs in the response plan emphasizes the importance of these activities in mitigating a significant cyber incident. Further, doing so ensures that the state is encapsulating the 14 core capabilities detailed in the NCIRP, such as access control and identify verification; cybersecurity; planning; and screening, search and detection.
- **Integrate National Guard resources (e.g., personnel) into the response plan:**[35] Colorado found that the National Guard "provided significant support to incident command, threat identification and analysis, and technical expertise."[36] Further, Colorado recommended that it establish prearranged contracts or memorandums of understanding with organizations like the National Guard to fill capacity gaps within the state's IT agency.

Cyber UCG and Cybersecurity Response Teams

- **Establish and create operational procedures for CRTs:** Preestablished CRTs could have the benefit of exercising across agencies and ingraining EM principles and procedures with IT personnel and other disciplines. Further, exercising or responding to insignificant cyber incidents may help the CRT identify and address operational gaps.
- **Create an auxiliary cybersecurity force of volunteers, akin to a volunteer fire department:** If a large-scale, significant cyber incident occurs, the state will most likely be limited in how many affected entities it could assist. States should consider creating CRTs composed of cybersecurity volunteers, such as the Michigan Cyber Civilian Corps (MiC3), who could be activated during a significant cyber incident response.[37] The MiC3 is a cadre of vetted, volunteer cybersecurity experts who can be activated alongside state IT employees during a cyber incident to provide response and recovery.

Conclusion

Strengthening state preparation for and response to a significant cyber incident is critical to achieving national resiliency. Significant cyber incidents could affect CI across state lines and stretch the federal government's ability to respond. In such a situation, states will need plans in place to ensure they are organized and prepared to respond without federal assistance. The NCIRP, the 15 plans identified and AARs provide the foundation for understanding how states can lead the way in preparing for, responding to and recovering from a significant cyber incident.

Michael Garcia
Senior Policy Analyst
Homeland Security and Public Safety Division
National Governors Association Center for Best Practices

Appendix

Table 2: Where Does the State Plan Reside?

State	Where does the plan reside within the state? How does it relate to the state's emergency operations plan?
Arizona[38]	An incident annex within the Arizona State Emergency Response and Recovery Plan.
Colorado[39]	Appendix to ESF 2.
Connecticut[40]	Annex to the State Response Framework.
Illinois[41]	Annex to the EOP called "Information and Cyber Security."
Maine[42]	Incident annex to the EOP.
Maryland[43]	Cyber disruption response activities integrated throughout the Consequence Management Operations Plan.
Massachusetts[44]	The plan is a separate ESF titled "ESF-17"; not an operational or tactical document.
Michigan[45]	Stand-alone document from the state's EOP; for data-collection purposes, viewed as an appendix.
Ohio[46]	Cyber incident response plan within ESF 2; although it is called an incident response plan, the plan dictates that the state's EM agency "assist in mitigating physical impacts."
Oregon[47]	Incident annex to the state's EOP; although called an incident response plan, the plan references mitigating and recovering from the physical impacts of a significant cyber incident.
South Carolina[48]	An appendix to the state's EOP; the primary focus of consequence management response and recovery efforts as identified in this plan are on the lifeline sectors of CI, which includes transportation, communications, water/wastewater, public health and energy. The plan also details specific roles and responsibilities for ESFs 2, 3, 8, 12 and 14.
Vermont[49]	The cyber annex is detailed as Incident Annex 5 within the state's EOP.
Washington[50]	Plan accompanies the Washington State Comprehensive Emergency Management Plan, which is based in part on a draft version of the NCIRP.
West Virginia[51]	An incident-specific annex to the state's EOP.
Wisconsin[52]	Annex within the state's EOP; created after the NCIRP.

Table 3: Which Threat Schema Does the Plan Use?

State	Which threat schema does the plan use?
Arizona[53]	Based on the 2010 draft NCIRP, the plan has four risk levels, ranging from severe to guarded. The plan also details six categories of cyber incident, with corresponding frequency of occurrence and areas of concern, including system fault, accident, disaster, computer crimes, cyberterrorism and act of war.
Colorado[54]	Uses the Multi-State Information Sharing Analysis Center's (MS-ISAC) security alert determination.
Connecticut[55]	Schema includes five levels, ranging from low to emergency, and provides a definition of the level, escalation criteria, de-escalation criteria, potential impact and the communications procedure; also discusses information-sharing protocols for a regional incident and the state associations Connecticut would engage during an incident.
Illinois[56]	None detailed, but notification to state agencies regarding cyber incidents will be carried out in accordance with the Illinois Department of Innovation & Technology (DoIT) Computer Security Incident Response Plan.
Maine[57]	Details three types of incidents: minor, major and disaster. The plan is activated when one of the following occurs: major incident or disaster; threat or incident involving state-level cyber CI; incident involving activation of state-level COOP or continuity of government (COG) plans; or at the request of a member of the cybersecurity incident response team (CSIRT), the director of the Maine Emergency Management Agency (EMA), TAG or the governor.
Maryland[58]	Details activities for steady-state and enhanced threat/hazard.
Massachusetts[59]	Uses five levels, ranging from Low (1) to Emergency (5), with an Emergency posing an imminent threat to life and safety, the provision of large-scale CI services or national or state government stability.
Michigan[60]	Does not use a threat schema but a risk assessment methodology that is conducted on the CI to determine the risk of an incident, if one were to occur.
Ohio[61]	None detailed.
Oregon[62]	Does not have a threat schema but details three levels of activation (standby, limited and full), with a full activation occurring when: • A localized emergency escalates, adversely affecting a larger area or jurisdiction and exceeding local response capabilities. • The Oregon Emergency Response System receives an alert from an official warning point or agency indicating a probable disaster or a local level disaster or emergency. • A governor issues a state of emergency. • Terrorist or weapons of mass destruction activities are occurring or imminent.

State	Which threat schema does the plan use?
	• An alert, site-area emergency, or general emergency is declared at the Hanford Site's Washington Nuclear Power Plant #2 (Washington State) or research reactors at Oregon State University or Reed College.
South Carolina[63]	None detailed; plan limited to South Carolina's consequence management response to and recovery from the physical effects of a significant cyber incident.
Vermont[64]	Plan has an escalation and notification matrix, with functional impact categories.
Washington State[65]	None detailed; state-level coordination of significant cyber incidents is triggered when the state EOC (SEOC) is activated after receiving a request for assistance related to the incident.
West Virginia[66]	None detailed; framework can be used in any incident with cyber-related issues, including significant cyber threats and disruptions, crippling cyberattacks against the internet or CI information systems, technological emergencies or declared disasters.
Wisconsin[67]	Uses the National Crime Information Center's Threat Schema, but Wisconsin also conducts its own assessment of the cybersecurity threat posed within the state and may increase the state's cybersecurity threat level independent of the federal government's assessment. Elevation of the cybersecurity threat level up to level 2 is at the direction of the Division of Enterprise Technology's (DET) administrator; elevation of the cybersecurity threat level above level 2 is at the direction of TAG. In the event of a credible threat or detection of an attack, TAG, the Wisconsin EM administrator or the DET administrator can activate incident response activities. Conditions that can trigger the incident response functions of this annex include (1) an incident involving activation of state-level COOP or COG plans; (2) a threat or incident involving state-level, cyber-critical infrastructure; (3) when requested by a local or tribal unit of government, the Department of Administration (DOA) DET management or the Department of Military Affairs (DMA) Wisconsin Emergency Management (WEM); (4) when directed by the DET administrator up to cybersecurity threat level 2 or TAG at cybersecurity threat level 3 or above.

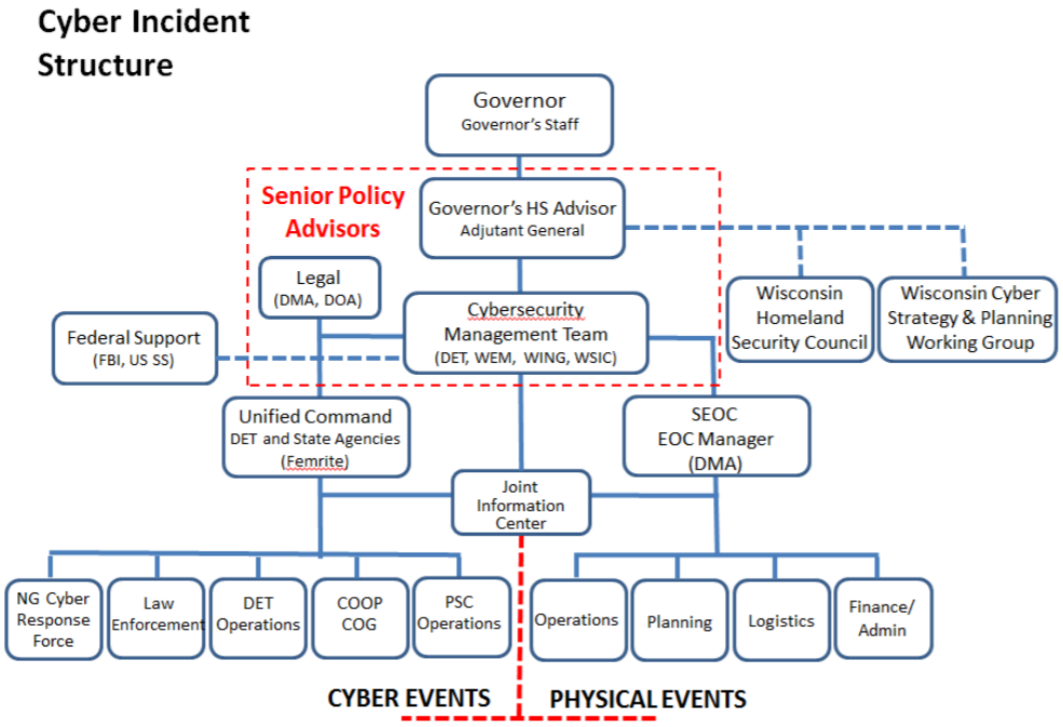
Table 4: Which are the Lead and Supporting Agencies?

State	Which is the lead agency? Which are the supporting agencies?
Arizona[68]	**Lead agencies:** Arizona Strategic Enterprise Technology (ASET), which includes Security, Privacy and Risk and the Arizona Security Operations Center (ASOC), and the Arizona ISAC Portal. **Supporting agencies:** Arizona Department of Emergency and Military Affairs (DEMA), Arizona Division of Emergency Management (ADEM), the Arizona National Guard, the Arizona Department of Homeland Security (ADOHS), the Arizona Department of Public Safety (ADPS) and the Arizona Counter Terrorism Information Center (ACTIC).
Colorado[69]	**Lead agency:** Colorado Office of Information Technology. **Supporting agencies:** All state agencies. The plan provides general R&Rs for primary agencies, which are entities with significant authority, roles, resources or capabilities. It also details R&R for support agencies, which are entities with specific capabilities or resources that support the primary agency in executing the cybersecurity ESF mission.
Connecticut[70]	**Lead agencies:** Connecticut Department of Administrative Services (DAS); the DAS Bureau of Enterprise Technology (BEST); and the Connecticut Department of Emergency Services and Public Protection (DESPP), Division of Emergency Management and Homeland Security (DEMHS). **Supporting agencies:** Connecticut chief cybersecurity risk officer; DESPP Division of Connecticut State Police (CSP), CSP Cyber Crimes Investigation Unit; DESPP Division of Scientific Services; DESPP Connecticut Intelligence Center (CTIC); DESPP Fire Prevention and Control Commission; Military Department; University of Connecticut; Connecticut state colleges and universities; Connecticut Department of Energy and Environment Protection, Public Utility Regulatory Authority. A cyber disruption task force (CDTF) will be established during an incident, and every lead and supporting agency will have at least one member on it; it will be led by the state CISO. The CDTF is activated at the direction of the governor, DESPP commissioner or deputy commissioner, or state EM director.
Illinois[71]	**Primary agency:** DoIT. **Supporting agencies:** Illinois State Police, Illinois EMA, Illinois National Guard (ILNG), Illinois Office of the Attorney General (OAG), Statewide Terrorism and Intelligence Center.
Maine[72]	**Lead agencies:** Maine Department of Defense, Veterans and Emergency Management (DVEM), Maine EMA; Maine Department of Administrative and Financial Services, Office of Information Technology (OIT).

State	Which is the lead agency? Which are the supporting agencies?
	Supporting agencies: Maine Department of Public Safety, Maine Information and Analysis Center (MIAC), Maine State Police Computer Crimes Unit (MSPCCU), Criminal Investigations Division; Maine DVEM, Maine Army National Guard (MENG); Maine Department of Administrative and Financial Services, Office of Risk Management; Maine Cyber Security Cluster. A CSIRT is formed when a cyber-related incident is detected. It includes the director of Maine EMA, OIT, the director of the MIAC, the MENG J6 and the Office of Risk Management.
Maryland[73]	The Consequence Management Operations Plan uses a whole-of-state approach; therefore, it is assumed that the Maryland EM Agency would lead, with all agencies assisting in response.
Massachusetts[74]	**Lead agencies:** Executive Office of Public Safety and Security (EOPSS), the Massachusetts Emergency Management Agency, the Massachusetts National Guard, the Massachusetts State Police, the Commonwealth Fusion Center and the Executive Office of Technology Services and Security. **Supporting agencies:** Massachusetts Department of Public Utilities, the Massachusetts Institute of Technology (MIT), Cybersecurity at MIT Sloan, IBM Security and RSA Security.
Michigan[75]	The Michigan Cyber Disruption Response Team (CDRT) is the coordinating structure for cyber disruption incidents. CDRT's leadership consists of representatives from the Michigan Department of Technology, Management and Budget (DTMB) and Michigan State Police. The chief security officer (CSO) acts as the CDRT chair, and the deputy director of the Emergency Management and Homeland Security Division (EMHSD) serves as the vice chair. CDRT's core group has state members from DTMB (including the Michigan ISAC), EMHSD, Michigan Cyber Command, the Intelligence Operations Center, Michigan National Guard, private-sector entities and others as necessary. Regional and national contacts are within CDRT, as well. Other actors include the Michigan Cyber Civilian Corps, the state's fusion center, federal entities and the Cyber Command Center within the Michigan State Police. The latter coordinates cyber first responders and develops strategies for criminal prosecution. See Figure 3 in the annex for CDRT's organizational chart.
Ohio[76]	**Lead agency:** Ohio DAS OIT. **Supporting agencies:** Ohio EMA; Ohio State Highway Patrol; Ohio Homeland Security (OHS); TAG Department, Ohio National Guard (OHNG).
Oregon[77]	**Lead agency:** Oregon DAS.

State	Which is the lead agency? Which are the supporting agencies?
	Supporting agencies: UCG created during an event, including Oregon DAS, the Oregon Military Department, other affected state agencies, LE and technology resources from the private and public sectors.
South Carolina[78]	A UCG will be established during an incident. The South Carolina Emergency Management Division is the lead agency for consequence management efforts in response to and recovery from the physical effects of a significant cyber incident. The South Carolina Law Enforcement Division (SLED) is the lead agency for criminal investigations. The SLED public information officer (PIO) will be the lead PIO for the overall response to the cyber event.
Vermont[79]	**Lead agencies:** Vermont Department of Information and Innovation (DII), DEMHS; DII and DEMHS will act jointly as EOC managers and conduct decision-making activities collaboratively. If the attack is focused on private-sector CI, the technical expertise will come from the National Guard Cyber Advisor Teams. **Supporting agencies:** Vermont State Police; fusion center; Vermont Criminal Justice Services, OIT; Vermont National Guard; Attorney General's Office.
Washington[80]	**Lead agencies:** Homeland Security Advisor, who is also TAG. **Supporting agencies:** A cyber UCG will be established and include the Washington CIO; the director of consolidated technology services; the director of EM; the state CISO; Seattle's CISO; the FBI; co-chair, Telecommunications & Energy; Affiliated Tribes of Northwest Indians; a representative of the University of Washington Center for Information Assurance; private industry/CIKR representatives (from each of the 18 sectors, depending on the specific nature of the incident); Washington State Emergency Management Division's Cyber Security manager; Washington National Guard Lead Cyber Planner; Washington State Patrol High Tech Crimes Unit representative; cyber intelligence analysts; Washington State Fusion Center; Cyber Incident Response Coalition and Analysis Sharing; and other organizations or vendors that participate in information sharing and assistance.
West Virginia[81]	**Lead agency:** West Virginia Division of Homeland Security and Emergency Management (WVDHSEM). **Primary supporting agencies:** West Virginia Office of Technology (WVOT) and West Virginia Intelligence Fusion Center. **Supporting agencies and organizations:** West Virginia Department of Military Affairs and Public Safety (WVDMAPS).
Wisconsin[82]	**Lead agencies:** Wisconsin DOA, DET; DMA, WEM. **Supporting agencies:** Wisconsin DMA, Wisconsin National Guard (WING); Wisconsin Department of Justice, Wisconsin Statewide Intelligence Center (WSIC). Please see Figure 2 for the organizational chart.

Figure 2: Wisconsin' Cyber Incident Structure



Abbreviations: NG = National Guard; PSC = Public Service Commission; SS = Secret Service.

Table 5: What are the R&Rs?

State	What are the roles and responsibilities?
Arizona[83]	**ASET:** Operates the ASOC and leads the state's government network cyber incident response; acts as the incident command; ensures development, training, mobilization and coordination of a state CIRT; and requests and coordinates the response of external cyber resources and organizations. **ADEM:** Operates the SEOC and coordinates state agency incident response. In a cyber incident, DEMA is the lead coordinating agency. Verifies that a cyber incident has occurred and requests activation of the annex from the governor; coordinates with ASET to develop a rapid assessment of the incident and determine appropriate, recommended protective actions; coordinates the state and federal (if required) response and recovery efforts and request for presidential declaration, if applicable. Coordinates short- and long-term recovery efforts with locals and tribes. **Arizona DOA:** Plans, directs, coordinates and implements protective monitoring measures for state information systems; plans and assists in the collection of electronic and video evidence; investigates computer criminal activity, computer fraud and abuse activities; and provides oversight to the statewide security assessment process. **ADOHS:** Provides a representative or liaison to SEOC as requested. **ADPS:** Leads state LEAs to coordinate and respond to cyber events, uses computer forensic teams to help identify evidence and examines computers and components. **ACTIC:** Coordinates inter- and intrastate information sharing.
Colorado[84]	In addition to detailing specific R&Rs, the plan details the organization's capabilities. Some of those capabilities are reflected here: **OIT:** Serves as lead state agency; issues notifications to its community describing the threat or hazard and any proactive measures to counter the effects of the cyber activity; and is decision maker for either taking the appropriate measures to halt the incursion or to allow the incursion to continue in an effort to gather forensics data and identify the perpetrator or gather evidence for prosecution. The same decision-making authority will be passed to a local jurisdiction if the state were to provide support to that jurisdiction. **Colorado DHSEM, Office of Emergency Management:** Leads consequence management portion of the incident and facilitates coordination of recovery efforts and communications. **OIT/DHSEM:** Establishes a single liaison with private sector entities involved in the restoration of services after an incident; recommends the SEOC activation level; provides recommendations to cabinet members; assesses the ongoing impacts of the incident; provides analysis of the extent and duration of incident; identifies requirements for consequence management. **DHSEM's Fusion Center (Colorado Information Analysis Center [CIAC]):** Conducts threat information sharing; assists in attributing the source of cyberattacks through DHSEM resources and the network of fusion centers; forensic analysis and support provided by OIT, CIAC and Colorado Bureau of Investigation (CBI) staff.

State	What are the roles and responsibilities?
	OIT and DHSEM CIAC: Analyze cyber vulnerabilities, exploits and attack methodologies; provide technical assistance; defend against attack; provide indications and warnings of potential threats, incidents and attacks. **CBI:** Investigative R&R. **Colorado Department of Military and Veterans Affairs (DMVA), Computer Network Defense:** DMVA may provide information assurance best practices, vulnerability assessment exercises, penetration testing and intrusion detection. DMVA's Computer Network Defense Team has the capabilities to provide cyber analysis capabilities, including forensic examination of networks and systems; threat assessment and unclassified adversary tactics, techniques and procedures; situation awareness and information sharing; incident mitigation; incident recovery; and training and education.
Connecticut[85]	The plan details prevention, mitigation, preparedness and response R&Rs. Only response R&R are detailed below. **DAS/BEST (for When a Cyber Disruption Event Occurs Within the State's Network):** Acts as the lead technical agency; works with CTIC; facilitates information sharing; activates all or part of the CDTF, which CIO leads; stands up the CSIRT or incident management team; assesses affected systems and networks, and develops a remediation and restoration plan; communicates status to relevant stakeholders; coordinates all IT personnel and resources in the response efforts; facilitates IT COOP/COG. **DESPP/DEMHS:** Serves as the lead coordination point for state response; activates all or part of the CDTF in consultation with other members; engages BEST as a technical specialist; recommends to the governor activation of the SEOC to coordinate response and recovery; working with the CDTF, develops a remediation and restoration plan; determines partial or full activation of the SEOC; communicates status reports to relevant stakeholders; conducts traditional EM responsibilities. **DESPP/CSP (When a Cyber Disruption Occurs Within the Public Safety Data Network, the Following Actions Can Be Taken):** Conducts investigations; recommends activation of the CDTF; develops a remediation and restoration plan; and communicates with appropriate stakeholders. If the effect on the public safety data network is not yet known, the following actions can be taken: Participates in the CDTF, and determines the scope of the disruption to see if the public safety data network is affected and ensures its protection. **CDTF:** Activated to determine appropriate actions to respond to and mitigate damage. During an incident that affects state computer systems, reports information to BEST CSIRT; conducts or cooperates with investigative duties; requests activation of the SEOC; monitors events and collects and shares information; provides situational awareness and subject matter expertise; recommends solutions for the SEOC during a response; coordinates IT-related intra- and interjurisdictional response activities; coordinates with the governor's unified command. **Connecticut Chief Cybersecurity Risk Officer:** Identifies critical partners, provides guidance on priorities; staffs or leads a task force as requested; and assists with messaging.

State	What are the roles and responsibilities?
	Connecticut Military Department: Performs incident response functions, such as assessment and remediation functions; reporting; and coordination with federal, state and local elements. **PURA:** Participates in the CDTF as requested; coordinates response to resource and assistance requests for matters pertaining to public utility operations. Other agencies could include DESPP Division of Scientific Services, DESPP Division of Statewide Emergency Telecommunications and DESPP Connecticut Commission on Fire Prevention and Control. Please see Figure 3 for communications flow for cybersecurity threats.
Illinois[86]	**DoIT:** Administers and manages the state's incident-handling efforts and coordinates as appropriate with community partners; categorizes cyber incidents and determines prioritization of efforts for state agencies; conducts and coordinates forensic analysis and attributes cyber incidents; identifies, assesses and prioritizes risks to inform prevention and protection activities; categorizes cyber incidents and determines prioritization of efforts for state agencies; notifies, activates, deploys, coordinates, implements and sustains the CSIRT; notifies the SEOC; assists state agencies in response to and recovery from cyber incidents; analyzes damage from cyber incidents that affect critical and lifeline infrastructure, the environment and public safety; coordinates with Illinois EMA to activate a joint information system; and coordinates with Illinois EMA to request implementation of the EOP and SEOC. **Illinois EMA:** Establishes strategic and operational command, coordination and control of state resources and supports organizations required for consequence management; coordinates with the DoIT liaison to determine the need to implement the Illinois EOP and activate the SEOC for consequence management efforts; and determines the appropriate level of activation for the SEOC. **State Police:** Assist in forensic analysis, attribution, investigation and adjudication of cyber incidents; coordinate and manage state LE activities; and conduct information-sharing activities through the fusion center. **Illinois OAG:** Coordinates with appropriate authorities for the prosecution of criminal cases brought by the state. **ILNG:** Assists in the analysis of incident intelligence, development of situational awareness and technical assistance to prevent, protect, respond to, recover from and mitigate the effects of a cyber incident; activates the Illinois General Assembly for external response assets with DoIT upon request and gubernatorial approval.
Maine[87]	The plan details prevention and protection activities. Only response activities are included. **OIT:** Serves as primary agency; identifies and coordinates support-function staffing requirements appropriate to the emergency situation, including coordination of the CSIRT; coordinates the response to requests for assistance from the affected agencies; assists in documentation preparation for departmental funding needs and developing priorities for state resource allocation; assists in coordinating and monitoring state-funded remediation efforts; obtains and compiles documentation necessary for effective and efficient strategy

State	What are the roles and responsibilities?
	management by Maine EMA SEOC staff; and, in coordination with the Maine EMA, develops, maintains and distributes this and any appropriate SOPs. **Maine EMA:** Activates the CSIRT; coordinates CSIRT/SEOC staffing and functioning; manages resources through ESFs, if the SEOC is activated; facilitates information sharing; supports actions and notifications to local, state and federal partners; declares emergency thresholds and expense reimbursement; and requests the MENG CRT. **MIAC:** Provides information-sharing activities and reports. **MSPCCU:** Supports and assists with the investigation and prosecution of computer security breaches. **MENG:** Capabilities could include network support and guidance to affected agencies, vulnerability assessment, cyber incident response and recovery actions, and equipment requests to maintain connectivity during a cyberattack. All National Guard missions will be requested by MEMA or the SEOC, then validated and approved by the MENG Joint Operations Center. **Maine Cyber Security Cluster:** This partnership with the University of Maine System has industry and academic resources to assist in a federal, state or local cyber-related emergency. Future capability will include faculty, students and a lab environment that will function as an education and prevention resource through training opportunities and vulnerability testing. **CSIRT:** Coordinates the response to any significant cyberevent that affects the state of Maine technologies; is activated when notified by the MEMA director or at the request of another permanent member.
Maryland[88]	The plan details all state agencies' response to all hazards. Therefore, only cyber-related responses are detailed below. **Maryland Department of IT:** Coordinates with the Maryland Joint Operations Center (JOC) for specific threats and hazards that have a cyber, electronic or communications infrastructure nexus; provides subject matter expertise for electronic infrastructure-specific threats or hazards that may affect or are affecting the state; activates the Maryland CRT if indicated and appropriate; coordinates with local and federal counterparts as appropriate; and coordinates enhanced threat/hazard operations specific to the electronic infrastructure sector. It takes the following measures to limit the impact to the state's electronic infrastructure, if dictated by actual or anticipated impact: • **During a Response:** Provides coordinated use of the state's communication and cybersecurity resources by facilitating the procurement of communication- and protection technology-related goods and services; activates the Maryland CRT as needed and appropriate; determines the extent of the cyber impact, recommends and executes remediation efforts, and prepares for recovery operations as needed. **Maryland National Guard:** Participates with the Maryland CRT as needed.
Massachusetts[89]	The ESF document is not a technical/operational document, but it does detail prevention and protection, preparedness, response and recovery actions. Prevention actions consist of cyber hygiene actions and other normal-state activities, while preparedness actions include maintaining points of contacts for the ESF, participating in exercises and developing

State	What are the roles and responsibilities?
	strategies to address key ESF issues. Response actions consist of initial and continuing response to cyber incidents, with the former consisting of assessing, monitoring and coordinating information and resources and the latter consisting of continued coordination with ESF agencies. Finally, recovery activities include replacing and restoring damaged or destroyed equipment and participating in an AAR. **EOPSS:** Convenes calls to discuss and assess the incident and further actions, and provides strategic guidance and leadership. **Massachusetts EMA:** Coordinates state response actions to the consequences of a cyber incident; coordinates recovery efforts; and communicates and coordinates with other entities involved in cyber incidents.
Michigan[90]	**CIO:** Works with Michigan State Police, the State Budget Office, the chief technology officer (CTO) and the CSO to identify related issues and effects; assists in remediation efforts; and communicates with high-level political officials and the media. **CTO:** Works with the CIO, CSO and Michigan State Police to remediate cybersecurity issues and establish the SEOC, with Michigan State Police coordinating mitigation and recovery activities. **CSO:** Leads response efforts with Michigan State Police or the incident commander; sets and alerts the state regarding the current threat posture; coordinates IT recovery activities; and coordinates remediation efforts from a cybersecurity event, among other activities. **Michigan State Police Emergency Management and Homeland Security Division:** Coordinates statewide response of the counties and municipalities; acts as the state's backup cybersecurity operations center. **National Guard Cyber Teams:** Combat cyberattacks and restore critical physical infrastructure; establish alternate forms of telecommunications; and assist with physical security. Not detailed in this document is the Michigan Cyber Civilian Corps, a vetted team of volunteers with cybersecurity credentials that can assist in responding to an event when the governor declares an emergency.
Ohio[91]	**OIT:** Provides staff to the SEOC; develops reporting mechanisms; develops a cyber-related resource manual; and provides resources and guidance to stakeholders and partners, among other activities. **EMA:** Assists in mitigating physical impacts; provides logistical support and SEOC management; and coordinates information flow, among other activities. **State Highway Patrol:** Serves as a liaison to LE at all levels and leads efforts to gather evidence. **OHS:** Provides intelligence support; coordinates tracking down information from divergent sources; and provides a clear picture of the incident. **OHNG:** Provides cyber incident response, as directed by the governor, regardless of scope or customer type; provides supplemental incident response personnel to DAS/OIT to help manage the incident; and relieves personnel and reduces staff fatigue, among other activities.

State	What are the roles and responsibilities?
Oregon[92]	**DAS:** Primary agency that notifies and requests assistance from support agencies; ensures financial and property accountability for Cyber Annex activities; plans for short- and long-term incident management; identifies new equipment or capabilities to prevent or respond to new threats; and responds directly to the officer in charge in the state emergency coordination center (ECC). If the governor determines that the emergency is related to computer or telecommunications systems, he or she may designate DAS as the lead agency, among other actions. **State Incident Response Team (SIRT):** Responds to information security incidents that potentially affect multiple agencies or that pose a significant threat to the state of Oregon; and coordinates interagency security incident response resources and communications during or about an information security incident that affects multiple agencies. The ECC, fusion center and supporting agencies' R&R are also identified but are general in nature. Other ESFs will be activated as needed, and the agencies identified in those ESFs will participate in responding to a cyberevent.
South Carolina[93]	Overall, the roles, responsibilities and activities will fall under "crisis management" and "consequence management." This framework can be implemented with or without the activation of the South Carolina EOP. **Crisis Management:** Measures to identify, acquire and employ resources to anticipate, prevent or mitigate a threat, including the forensic work to identify the adversary. SLED is the lead agency for crisis management response. **Consequence Management:** Measures taken to manage the physical effects of the crisis. The South Carolina Emergency Management Division is the lead agency for the consequence management response to a significant cyber incident. These activities are conducted by multiple agencies and coordinated by EM. **SEOC:** Serves as the central coordination point for consequence management response and is activated based on the level of requested support, the need to gain situational awareness of the incident or on the direction of the governor. This plan is unique because it details specific roles and responsibilities for ESF 1, 2, 3, 8, 12 and 14.
Vermont[94]	**DII:** Coordinates the execution of the annex; coordinates statewide IT damage and assessment; disseminates cyber-related threat, response and recovery information concerning cyber events that target the state IT enterprise; Identifies the cause of a cyber incident, isolates the risks, removes the problem from a system and prepares the system for recovery, and determines when the system can safely be restored; and supports state agencies experiencing a cyber incident. **DEMHS:** Serves as co-manager of the EOC; coordinates cyber response resource management; coordinates emergency public information; identifies cyber-related CI; and coordinates SEOC staffing and operations. **The Vermont Cyber Response Assessment Board (CRAB):** See Table 6 for more information.

State	What are the roles and responsibilities?
	LEAs: Maintains law and order during social repercussion resulting from the cyber event; gathers intelligence and disseminates warnings; directs criminal investigation of a cyber event or coordinates with federal entities; supports communications and IT; and supports cyberterrorist incident activities. **Fusion Center:** Provides specific event assessment and warning dissemination to DII or relevant CI sector partners, among other activities. **National Guard:** Validates, approves and coordinates the mission with the DEMHS and the director of operations for military support; and advises and assists the state emergency response effort by participating in the CRAB and using the Cyber Assistance Team.
Washington[95]	**HSA:** Manages a significant cyber incident, establishes a cyber UCG and reports directly to the governor. **EM Division:** Ensures that the state is prepared to deal with any disaster or emergency by administering the program for EM delineated by the HSA; coordinates the state's response to any disaster or emergency. **SEOC:** Ensures overall coordination of significant cyber incident management and resource-allocation activities; and coordinates external affairs activities. **Washington State Fusion Center:** Facilitates information sharing and may host the cyber UCG. **Washington State Patrol:** Coordinates the initiation of cybercrime investigations with appropriate state and local LEAs and support from federal partners. **Security Operations Center:** Leads the coordination and response efforts in assessing and managing cyber incidents that affect state government networks; determines the level of response required to respond to incidents; directs the use of agency resources to minimize incident exposure; and ensures that appropriate enterprise protection controls are deployed. **CIKR Sector-Specific Agencies:** Develop a process to facilitate real-time cyber incident notification within their respective sectors, and provide mechanisms for reporting this information.
West Virginia[96]	**WVDHSEM Director:** Provides general guidance for emergency operations, including the response to cyber incidents, in coordination with WVOT; identifies cyber-related CIKR; and performs traditional EM response activities. **WVOT:** Monitors the state network at all times for suspicious cyber activity; coordinates IT damage and assessment; disseminates cyber-related information through multiple means; identifies the cause of a cyber incident and isolates the risk; when appropriate, removes the problem from a system and prepares that system for recovery; determines when the system can safely be restored; coordinates cybertraining and education of state sectors; supports and communicates with state agencies and school systems experiencing a cyber incident on their respective network; assists local, state and federal LE with cyber-related investigations and data analysis; establishes and maintains a COOP plan for reestablishing access to hosted services following a disaster; and reports any suspicious activity to the WVDHSEM when a cyber incident significantly threatens the state network.

State	What are the roles and responsibilities?
	WVDMAPS: Supports the lead agency in response to a cyber incident; protects CI; supports communications and IT; coordinates with WVDHSEM and WVOT to provide overall direction of cyberterrorist incident response activities; assists local and federal LEAs with cyber-related investigations and data analysis; uses U.S. Army and U.S. Air Force personnel expertise through a cyberliaison response capability; and provides response augmentation in accordance with proper legal authority.
Wisconsin[97]	Wisconsin describes general R&R and specific R&R for each of six threat levels. Level 0, or steady-state operations, are not included in the R&R below. **DMA/WEM:** Serves as the lead coordinating agency during a state of emergency declared by the governor; in a cyber- or telecommunications-related incident, however, the governor may designate DOA/DET as the lead agency responding as follows: • **Threat Level 1:** The WEM processes initial notification from the affected entity or notifying agency per SOP; receives notice of and monitors potential deployments of Wisconsin CRT assets; and monitors the affected entity activity and other potential effects. • **Threat Level 2:** In addition to activities in Threat Level 1, may create an incident site in the Web EOC to document the life cycle of the incident; receives and monitors potential deployments of Wisconsin CRT assets; prepares to support the affected agency with COOP efforts, if needed; may establish the Business EOC; and considers informing the Federal Emergency Management Agency (FEMA) Region 5 Regional Response Coordinating Center. • **Threat Level 3:** In addition to activities in Threat Levels 1 and 2, may activate the SEOC and notify WEM regional directors. • **Threat Level 4:** Activities in Threat Levels 1-3. • **Threat Level 5:** Activities in Threat Levels 1-3. **DOA/DET (Includes CISO):** May be designated as the lead agency during a cyber state of emergency providing the following response: • **Threat Level 1:** Begins to assess potential impacts to the state of Wisconsin IT enterprise; may direct the deployment of a Wisconsin CRT to the affected entity. • **Threat Level 2:** In addition to actions in Threat Level 1, consults with TAG (or a representative) on recommended courses of action; ensures that agency CISOs successfully complete remediation activities; and begins to assess potential impacts to the state of Wisconsin's IT enterprise and works to mitigate the process or systems affected by the event. • **Threat Level 3:** In addition to activities in Threat Levels 1 and 2, joins TAG for meetings with CRT and determines whether to initiate COOP measures for DET. • **Threat Level 4:** In addition to activities in Threat Levels 1-3, provides direction and priorities to the state of Wisconsin IT enterprise; may select a special focus on specific malicious threats or request that the Wisconsin Cyber Strategic and Planning Working Group (WCSPWG) convenes to discuss particular impacts of the emerging threat. • **Threat Level 5:** In addition to activities in Threat Levels 1-4, begins estimates of recovery requirements to the state of Wisconsin IT enterprise; may direct the deployment of multiple Wisconsin CRTs to the affected entity.

State	What are the roles and responsibilities?
	Wisconsin Department of Justice (DOJ)/WSIC: Coordinates information sharing among DET and WEM; state, local and tribal (SLT) LEAs; and other units of government. WSIC also coordinates information sharing with affected private-sector entities; the U.S. intelligence community, including U.S. DHS and its subordinate units; and with federal LEAs: • **Threat Level 1:** Continue general intelligence activities. • **Threat Level 2:** Establish a phone conference with the CISO, the Wisconsin JOC and the affected entity to communicate suspected origins, effects, current actions and next steps; notify state partner agencies per SOP; continue broad surveillance of cyberthreat spectrum and receive updates or information from deployed Wisconsin CRT assets; explore significant or potential indicators of compromise that may indicate a broadening of the threat and provide analysis of potential future targets; and may involve the Southeastern Wisconsin Threat Analysis Center. • **Threat Level 3:** In addition to activities in Threat Level 2, meet to be a part of a CMT and bring fusion center-specific content. • **Threat Level 4:** Same as activities in Threat Levels 2 and 3. • **Threat Level 5:** Same as activities Threat Levels 2 and 3, and update the Senior Policy Advisory Group (SPAG). **DMA/WING (Including JOC and the Defensive Cyberspace Operations Element):** WING has a CRT that may be deployable upon supportable mission analysis under applicable laws and regulatory parameters: • **Threat Level 1:** Monitor deployment of Wisconsin CRT assets in the state; track for potential future inclusion in the Wisconsin User-Defined Operating Picture; brief TAG on developments of the event, and consult with the Wisconsin CISO on recommended courses of action; and notify TAG of any deployment of a Wisconsin CRT. The Wisconsin JOC may lend assistance to other Wisconsin CRTs for liaison officer (LNO) duties or initial investigation of a cyber event. • **Threat Level 2:** Same as activities Threat Level 1. • **Threat Level 3:** Including activities threat Level 1, plan a mission support package and begin assessment of sustained, prolonged operations. • **Threat Level 4:** Including activities Threat Levels 1 and 3, at TAG's command and participate in meetings with the WCSPWG. • **Threat Level 5:** Same as activities Threat Levels 1, 3 and 4. **Adjutant General (Also HSA):** Serves lead advisor for cybersecurity matters, but the DET administrator is the state alternate for the point of contact. • **Threat Level 1:** The TAG does not become involved until Threat Level 2. • **Threat Level 2:** May direct the deployment of a CRT and convene the SPAG. • **Threat Level 3:** Same activities as Threat Level 1 and 2; maintain situational awareness of the event, and consult with the CISO on recommended courses of action; may direct a conference call or meeting with affected sectors of WCSPWG. **SPAG:** When a significant cyber event occurs that affects SLT systems, critical infrastructure or both in Wisconsin and the governor has not designated DOA/DET as the lead agency, the response effort will be led by TAG as chair of the SPAG, which consists of select members of the Wisconsin Cyber Management Team (CMT), DOA and DMA legal personnel.

State	What are the roles and responsibilities?
	CMT: Resides within the SPAG; may consist of personnel from DET, WSIC, WEM, WING, federal agencies and owners of affected systems; makes recommendations to the SPAG with regard to decision support involving primary and coordinating agency decisions in significant cyber incidents: • **Threat Level 1:** May be requested by the affected entity. • **Threat Level 2:** May be requested by the affected entity. • **Threat Level 3:** Meet to ascertain boundaries of the event and proscribe immediate actions based on size and scope. • **Threat Level 4:** Same as Threat Levels 1-3; determine recurrence of meetings. • **Threat Level 5:** Same as Threat Levels 1-4 . **WCSPWG.** Consists of subject matter experts from the public and private sector responsible for advising on preparation, response to and recovery from large-scale or long-duration cyber disruptions that affect Wisconsin's CI or other major assets and is responsible for continuing broad analysis of existing cyber response plans, risk assessments and knowledge sharing between and among members. During a disruption, the CMT may mobilize members of this group to act in an advisory capacity and analyze the immediate and long-term impacts of the disruption on CI in Wisconsin. Members may also be tasked with prescribing an order of recovery for affected sectors and systems as follows: • **Threat Level 1:** WCSPWG becomes involved in threat leve 2. • **Threat Level 2:** Assistance may be requested based on specific events. • **Threat Level 3:** May be convened at the CMT's request. • **Threat Level 4:** Convened at a time and place chosen by TAG or the lead agency, and assess risks and prescribe immediate actions for incident management. • **Threat Level 5:** Meet on a recurring basis to provide input to the CMT based on the event or incident. **CRTs:** Wisconsin has facilitated the establishment of five CRTs. The state CISO, as executive agent for the SLT CMTs, is responsible for training, certification, proficiency standards and validation criteria. The CISO incorporates FEMA standards for team membership and works cooperatively with DMA/WEM for training and credentialing of teams and individuals, respectively: • **Threat Level 1:** All or a portion of a team may be activated and act as initial liaison to investigate a threat in a government or private-sector entity; teams or LNOs pass back any forensic evidence to other teams and Wisconsin DOJ/WISC forensics. If any criminal activity is suspected, notification of WISC is mandated. • **Threat Level 2:** Same activities as Threat Level 1. • **Threat Level 3:** Same activities as in Threat Levels 1 and 2; team may be activated and instruct the initial liaison to investigate a threat in a government or private-sector entity. • **Threat Level 4:** Same activities as in Threat Levels 1-3. • **Threat Level 5:** Same activities as in Threat Levels 1-4. **End Use (Client):** Individual system owners are responsible for training their subordinates in proper and appropriate uses of equipment, software and networks. In a cyberattack, system

State	What are the roles and responsibilities?
	owners bear ultimate responsibility for equipment and network disruption and loss or exfiltration of data involving their computers, servers and network. **Local LEA:** Responsible for assisting in local investigations.

Figure 2: Connecticut's Communications Flow for Cybersecurity Threats

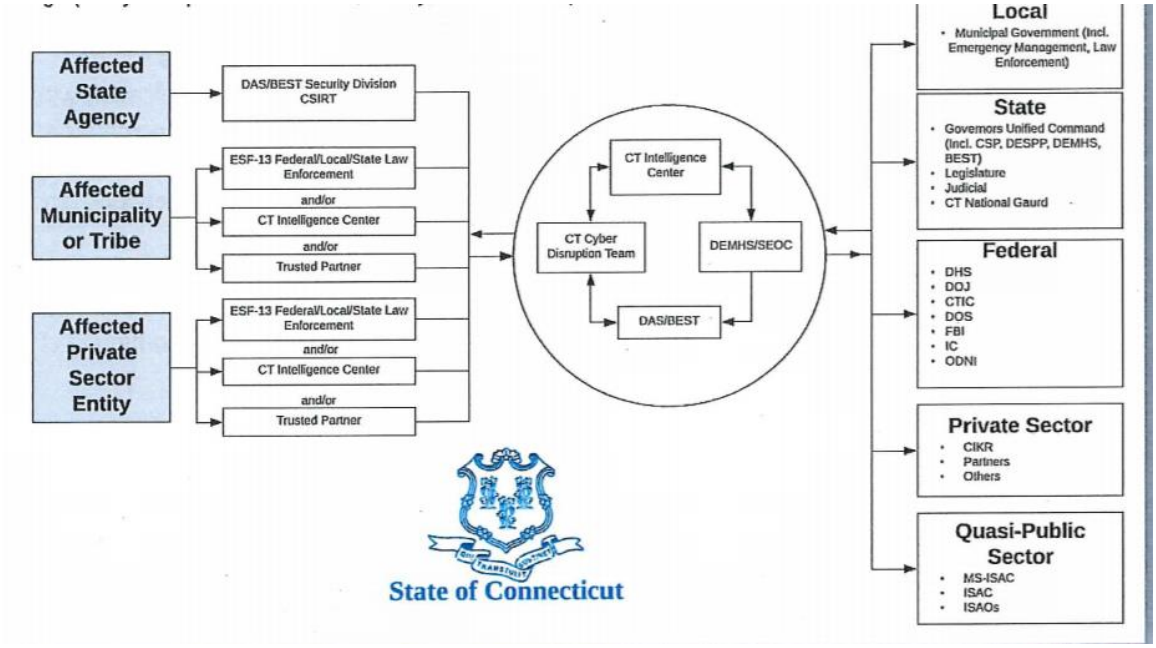


Table 6: Has a UCG or CRT Been Activated?

State	Has a UCG or CRT been activated?
Arizona[98]	ASET will operate a state CSIRT.
Colorado[99]	When an event occurs, a NIMS unified command structure will be established to coordinate the actions necessary for rapid identification, information exchange, response and remediation to mitigate the damage the cyber event has caused. The unified command will consist of the OIT, the Colorado Division of Homeland Security and Emergency Management (DHSEM), CBI and technology resources from the private and public sectors.
Connecticut[100]	A UCG will be established in addition to a cyber disruption task force. See Table 5 for more information.
Illinois[101]	A UCG would be established per NIMS ICS. Will deploy computer security IRTs whose R&R and composition are not included in the response plan.
Maine[102]	Yes, a CSIRT is created. See Table 4 for composition and Table 5 for R&R.
Maryland[103]	A CRT is established, but the plan does not detail its composition or R&R.
Massachusetts[104]	None detailed, but any activation of an ESF would potentially trigger the creation of a UCG.
Michigan[105]	Yes, the CDRT conducts preparation, response and recovery operations. See Table 5 and Figure 4 for more information.
Ohio[106]	None detailed, but any activation of an ESF would potentially trigger the creation of a UCG.
Oregon[107]	Yes. See Table 4 for more information about the SIRT.
South Carolina[108]	Yes, a UCG is established. See Table 4 for more information.
Vermont[109]	The CRAB will coordinate the response to any significant cyber event that affects state or private technologies. The CRAB consists of DEMHS, the director of the fusion center, the CISO and the National Guard Director of Military Support: • CRAB members will use their own authority to assist response activities. • Any permanent member of the CRAB can convene the CRAB in response to an identified threat or hostile activity. • CRAB notification will be determined through a dialogue between the DEMHS watch officer and the fusion center and will use the following criteria: (1) ICS supervisory control and data acquisition intrusion or attack such that system control is lost within the water, energy, dam, nuclear, chemical, health care or transportation sectors; (2) compromise of the state IT enterprise; (3) compromise of sensitive defense industrial information; and (4) compromise of state internet service providers. • During a significant cyber incident, the CRAB will provide guidance to leaders in the SEOC. See Figure 5 for more information.
Washington[110]	Yes. State-level coordination of significant cyber incidents is triggered when the SEOC is activated after receiving a request for assistance related to the incident. At that point,

State	Has a UCG or CRT been activated?
	the significant cyber incident will be monitored and coordinated through the SEOC under the guidance of the cyber UCG.
West Virginia[111]	A UCG is presumed to be established because the NIMS is followed.
Wisconsin[112]	Yes. See Table 4 for more information.

Figure 4: Michigan's CDRT's Organizational Chart

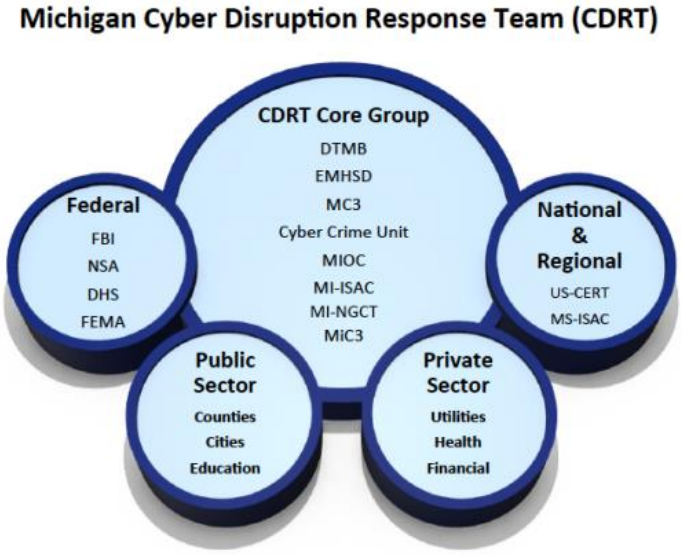
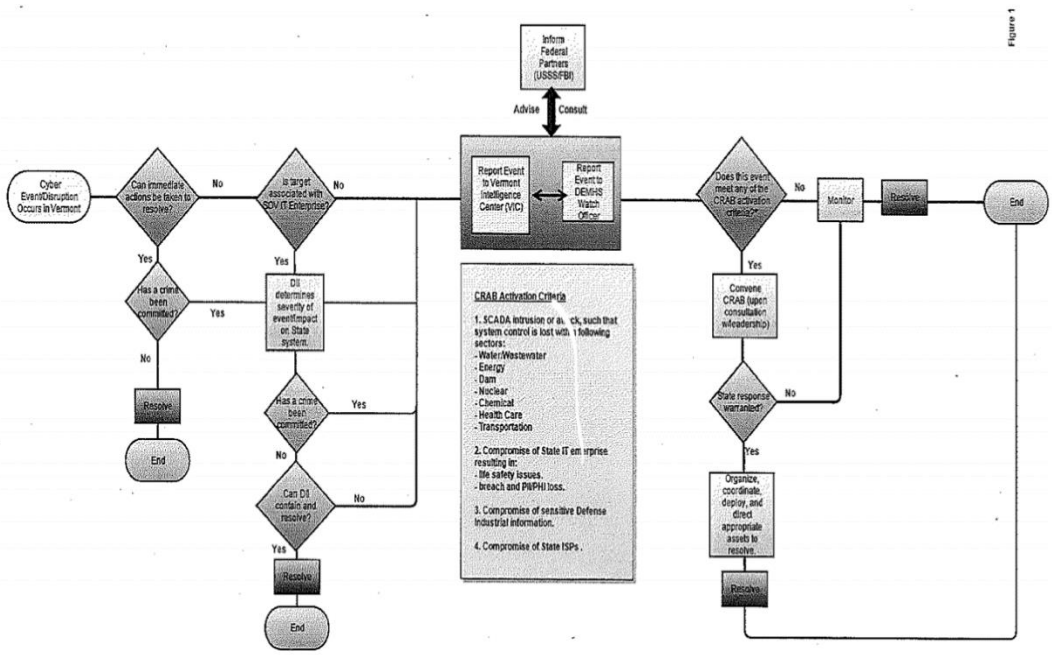


Figure 5: Vermont's CRAB Notification Procedures



[1] Finkle, J. (2016, November 28). San Francisco public transit system hit in ransomware attack. *Reuters.* Retrieved from https://www.reuters.com/article/us-california-cyber/san-francisco-public-transit-system-hit-in-ransomware-attack-idUSKBN13N1LN

[2] Leovy, J., & D'Angelo, A. (2017). Maersk's L.A. port terminal remains closed after global cyberattack. *The Los Angeles Times.* Retrieved from https://www.latimes.com/business/technology/la-fi-maersk-cyber-attack-20170629-story.html

[3] Colorado Department of Transportation. (2018, July 17). *CDOT cyber incident: After-action report.* Retrieved from https://www.colorado.gov/pacific/dhsem/atom/129636

[4] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 8). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[5] Brown, R. (2012, November 20). South Carolina offers details of data theft and warns it could happen elsewhere. *The New York Times.* Retrieved from https://www.nytimes.com/2012/11/21/us/more-details-of-south-carolina-hacking-episode.html; Shain, A. (2018, December 31). SC still fixing security after big data breach but ends victim credit monitoring. *The Post and Courier (Charleston).* Retrieved from https://www.postandcourier.com/politics/sc-still-fixing-security-after-big-data-breach-but-ends/article_0c48d0ee-fa84-11e8-ba6f-9f937355756e.html

[6] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 8). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[7] Perlroth, N., & Krauss, C. (2018, March 15). A cyberattack in Saudi Arabia had a deadly goal. Experts fear another try. *The New York Times.* Retrieved from https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

[8] Both plans have links to their respective state EOPs.

[9] Federal Emergency Management Agency. (2019, May 7). National Incident Management System. Retrieved from https://www.fema.gov/national-incident-management-system

[10] Obama White House Archive. (2016, July 26). *Presidential Policy Directive—United States cyber incident coordination* [press release]. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[11] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 8). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[12] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 13). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[13] The Affected Entity Response activities are used when a federal agency is affected. Presumably, the same would be true for an SLTT or private entity.

[14] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan.* Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[15] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 16). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[16] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 16). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[17] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 16). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[18] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 17). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[19] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 17). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[20] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 17). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[21] Obama White House Archive. (2016, July 26). *Presidential Policy Directive—United States cyber incident coordination* [press release]. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[22] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 27, 33). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[23] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 33). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[24] State of Wisconsin Homeland Security Council. (2015, October 30). *Wisconsin Cyber Disruption Response Strategy: Protecting critical infrastructure and systems of Wisconsin.* Retrieved from https://det.wi.gov/Documents/Cyber%20Disruption%20Response%20Strategy%20Plan%20Revised%2010_16.pdf

[25] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 28). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf; Colorado Department of Transportation. (2018, July 17). *CDOT cyber incident: After-action report.* Retrieved from https://www.colorado.gov/pacific/dhsem/atom/129636

[26] Colorado Department of Transportation. (2018, July 17). *CDOT cyber incident: After-action report* (page 7). Retrieved from https://www.colorado.gov/pacific/dhsem/atom/129636

[27] Colorado Department of Transportation. (2018, July 17). *CDOT cyber incident: After-action report.* Retrieved from https://www.colorado.gov/pacific/dhsem/atom/129636

[28] Colorado Department of Transportation. (2018, July 17). *CDOT cyber incident: After-action report.* Retrieved from https://www.colorado.gov/pacific/dhsem/atom/129636

[29] State of Michigan Executive Office. (2015, October 25). *Cyber Disruption Response Plan* (page 21). Retrieved from https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf

[30] State of Michigan Executive Office. (2015, October 25). *Cyber Disruption Response Plan* (page 20). Retrieved from https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf

[31] Colorado Department of Transportation. (2018, July 17). *CDOT cyber incident: After-action report* (page 8). Retrieved from https://www.colorado.gov/pacific/dhsem/atom/129636

[32] Colorado Department of Transportation. (2018, July 17). *CDOT cyber incident: After-action report.* Retrieved from https://www.colorado.gov/pacific/dhsem/atom/129636

[33] Meet the threat: States confront the cyber challenge. 2016–17 NGA Chair's Initiative: Memo on state cybersecurity governance bodies. 2016. Retrieved from https://ci.nga.org/files/live/sites/ci/files/1617/docs/TaskForceMemoFinal.pdf

[34] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan* (page 16). Retrieved from https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[35] Colorado Department of Transportation. (2018, July 17). *CDOT cyber incident: After-action report.* Retrieved from https://www.colorado.gov/pacific/dhsem/atom/129636

[36] Colorado Department of Transportation. (2018, July 17). *CDOT cyber incident: After-action report* (page 7). Retrieved from https://www.colorado.gov/pacific/dhsem/atom/129636

[37] For more information about establishing a volunteer CRT, please see Garcia, M. (2017). Building a cyber civilian corps. Retrieved from https://ci.nga.org/files/live/sites/NGA/files/pdf/2018/HSPS/MiC3%20Memo%20(1).pdf

[38] Arizona Department of Emergency and Military Affairs. (2017, February 8). *Arizona State Emergency Response and Recovery Plan.* Retrieved from https://dema.az.gov/sites/default/files/publications/EM-PLN_SERRP_2017_FINAL_Feb08_2017.pdf

[39] Colorado Division of Homeland Security & Emergency Management. (2016, November). *Colorado Hazard and Incident Response and Recovery Plan.* Retrieved from https://www.colorado.gov/pacific/dhsem/state-eop

[40] State of Connecticut. (2018, August). *Cyber Disruption Response Plan.* Retrieved from https://portal.ct.gov/-/media/DEMHS/_docs/Cyber-Disruption-Response-Plan-Signed-Oct-2018.pdf?la=en

[41] State of Illinois. (2017, March 31). *Illinois Emergency Operations Plan: Annex 22—Information and cybersecurity.* Retrieved from https://www2.illinois.gov/iema/Preparedness/Documents/IEOP/Annex22.pdf

[42] State of Maine. (2016, May 26). *Emergency Operations Plan—Incident annex 3: Cyber incident.* Retrieved from http://www.maine.gov/tools/whatsnew/attach.php?id=732508&an=1

[43] Maryland Emergency Management Agency. (2019, January). *Consequence Management Operations Plan.* Retrieved from https://mema.maryland.gov/Documents/Maryland_Consequence_Management_Operations_Plan%202.0_January%202019_FINAL%201.pdf

[44] Commonwealth of Massachusetts. (2019). *Comprehensive Emergency Management Plan.* Retrieved from https://www.mass.gov/lists/comprehensive-emergency-management-plan

[45] State of Michigan Executive Office. (2015, October 25). *Cyber Disruption Response Plan* (page 21). Retrieved from https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf

[46] Ohio Department of Administrative Services, Office of Information Technology. (2018, March). *Emergency Operations Plan. Emergency Support Function #2: Communications and information technology. Tab B—Cyber Incident Response Plan.* Retrieved from https://ema.ohio.gov/Documents/Ohio_EOP/EOP_Overview/ESF-2%20-%20Tab%20B%20-%20Cyber%20Incident%20Response%20Plan%20-%202018.pdf

[47] State of Oregon. (2015). *Emergency Operations Plan. Incident annex 10—Cyber security.* Retrieved from https://www.oregon.gov/oem/Documents/2015_OR_eop_ia_10_cyber.pdf

[48] South Carolina Emergency Management Division. (2018, July). *South Carolina Cyber Incident Consequence Management Plan. Appendix 16 to the South Carolina Emergency Operations Plan.* Retrieved from https://www.scemd.org/media/1367/appendix-16-sc-cyber-incident-consequence-managment-plan.pdf

[49] Vermont Emergency Management. (2016, May). *State of Vermont Emergency Operations Plan. Incident annex 5: Cyber annex.* Retrieved from https://vem.vermont.gov/sites/demhs/files/pdfs/plans/state/Incident%20Annex%205_Cyber%20Incident_2016_06.pdf

[50] Washington Military Department. (2015, March). *Washington state significant cyber incident annex to the Washington State Comprehensive Emergency Management Plan. Annex D.* Retrieved from https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf

[51] West Virginia Department of Homeland Security and Emergency Management. (2016, January). *Emergency Operations Plan. Incident specific annex 3: Cyber incident response.* Retrieved from http://dhsem.wv.gov/Resources/Documents/WV%20EOP%202016/IS%2003%20-%20Cyber%20FINAL%201-6-16.pdf

[52] State of Wisconsin Department of Military Affairs, Wisconsin Emergency Management. (2017, November). *Wisconsin Emergency Response Plan: Emergency Support Functions & incident specific annexes.* Retrieved from https://dma.wi.gov/DMA/divisions/wem/preparedness/2017_WERP(Full37M).pdf

[53] Arizona Department of Emergency and Military Affairs. (2017, February 8). *Arizona State Emergency Response and Recovery Plan.* Retrieved from https://dema.az.gov/sites/default/files/publications/EM-PLN_SERRP_2017_FINAL_Feb08_2017.pdf

[54] Colorado Division of Homeland Security & Emergency Management. (2016, November). *Colorado Hazard and Incident Response and Recovery Plan.* Retrieved from https://www.colorado.gov/pacific/dhsem/state-eop

[55] State of Connecticut. (2018, August). *Cyber Disruption Response Plan.* Retrieved from https://portal.ct.gov/-/media/DEMHS/_docs/Cyber-Disruption-Response-Plan-Signed-Oct-2018.pdf?la=en

[56] State of Illinois. (2017, March 31). *Illinois Emergency Operations Plan: Annex 22—Information and cybersecurity.* Retrieved from https://www2.illinois.gov/iema/Preparedness/Documents/IEOP/Annex22.pdf

[57] State of Maine. (2016, May 26). *Emergency Operations Plan—Incident annex 3: Cyber incident.* Retrieved from http://www.maine.gov/tools/whatsnew/attach.php?id=732508&an=1

[58] Maryland Emergency Management Agency. (2019, January). *Consequence Management Operations Plan.* Retrieved from https://mema.maryland.gov/Documents/Maryland_Consequence_Management_Operations_Plan%202.0_January%202019_FINAL%201.pdf

[59] Commonwealth of Massachusetts. (2019). *Comprehensive Emergency Management Plan.* Retrieved from https://www.mass.gov/lists/comprehensive-emergency-management-plan

[60] State of Michigan Executive Office. (2015, October 25). *Cyber Disruption Response Plan* (page 21). Retrieved from https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf

[61] Ohio Department of Administrative Services, Office of Information Technology. (2018, March). *Emergency Operations Plan. Emergency Support Function #2: Communications and information technology. Tab B—Cyber Incident Response Plan.* Retrieved from https://ema.ohio.gov/Documents/Ohio_EOP/EOP_Overview/ESF-2%20-%20Tab%20B%20-%20Cyber%20Incident%20Response%20Plan%20-%202018.pdf

[62] State of Oregon. (2015). *Emergency Operations Plan. Incident annex 10—Cyber security.* Retrieved from https://www.oregon.gov/oem/Documents/2015_OR_eop_ia_10_cyber.pdf

[63] South Carolina Emergency Management Division. (2018, July). *South Carolina Cyber Incident Consequence Management Plan. Appendix 16 to the South Carolina Emergency Operations Plan.* Retrieved from https://www.scemd.org/media/1367/appendix-16-sc-cyber-incident-consequence-managment-plan.pdf

[64] Vermont Emergency Management. (2016, May). *State of Vermont Emergency Operations Plan. Incident annex 5: Cyber annex.* Retrieved from https://vem.vermont.gov/sites/demhs/files/pdfs/plans/state/Incident%20Annex%205_Cyber%20Incident_2016_06.pdf

[65] Washington Military Department. (2015, March). *Washington state significant cyber incident annex to the Washington State Comprehensive Emergency Management Plan. Annex D.* Retrieved from https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf

[66] West Virginia Department of Homeland Security and Emergency Management. (2016, January). *Emergency Operations Plan. Incident specific annex 3: Cyber incident response.* Retrieved from http://dhsem.wv.gov/Resources/Documents/WV%20EOP%202016/IS%2003%20-%20Cyber%20FINAL%201-6-16.pdf

[67] State of Wisconsin Department of Military Affairs, Wisconsin Emergency Management. (2017, November). *Wisconsin Emergency Response Plan: Emergency Support Functions & incident specific annexes.* Retrieved from https://dma.wi.gov/DMA/divisions/wem/preparedness/2017_WERP(Full37M).pdf

[68] Arizona Department of Emergency and Military Affairs. (2017, February 8). *Arizona State Emergency Response and Recovery Plan.* Retrieved from https://dema.az.gov/sites/default/files/publications/EM-PLN_SERRP_2017_FINAL_Feb08_2017.pdf

[69] Colorado Division of Homeland Security & Emergency Management. (2016, November). *Colorado Hazard and Incident Response and Recovery Plan.* Retrieved from https://www.colorado.gov/pacific/dhsem/state-eop

[70] State of Connecticut. (2018, August). *Cyber Disruption Response Plan.* Retrieved from https://portal.ct.gov/-/media/DEMHS/_docs/Cyber-Disruption-Response-Plan-Signed-Oct-2018.pdf?la=en

[71] State of Illinois. (2017, March 31). *Illinois Emergency Operations Plan: Annex 22—Information and cybersecurity.* Retrieved from https://www2.illinois.gov/iema/Preparedness/Documents/IEOP/Annex22.pdf

[72] State of Maine. (2016, May 26). *Emergency Operations Plan—Incident annex 3: Cyber incident.* Retrieved from http://www.maine.gov/tools/whatsnew/attach.php?id=732508&an=1

[73] Maryland Emergency Management Agency. (2019, January). *Consequence Management Operations Plan.* Retrieved from https://mema.maryland.gov/Documents/Maryland_Consequence_Management_Operations_Plan%202.0_January%202019_FINAL%201.pdf

[74] Commonwealth of Massachusetts. (2019). *Comprehensive Emergency Management Plan.* Retrieved from https://www.mass.gov/lists/comprehensive-emergency-management-plan

[75] State of Michigan Executive Office. (2015, October 25). *Cyber Disruption Response Plan* (page 21). Retrieved from https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf

[76] Ohio Department of Administrative Services, Office of Information Technology. (2018, March). *Emergency Operations Plan. Emergency Support Function #2: Communications and information technology. Tab B—Cyber Incident Response Plan.* Retrieved from https://ema.ohio.gov/Documents/Ohio_EOP/EOP_Overview/ESF-2%20-%20Tab%20B%20-%20Cyber%20Incident%20Response%20Plan%20-%202018.pdf

[77] State of Oregon. (2015). *Emergency Operations Plan. Incident annex 10—Cyber security.* Retrieved from https://www.oregon.gov/oem/Documents/2015_OR_eop_ia_10_cyber.pdf

[78] South Carolina Emergency Management Division. (2018, July). *South Carolina Cyber Incident Consequence Management Plan. Appendix 16 to the South Carolina Emergency Operations Plan.* Retrieved from https://www.scemd.org/media/1367/appendix-16-sc-cyber-incident-consequence-managment-plan.pdf

[79] Vermont Emergency Management. (2016, May). *State of Vermont Emergency Operations Plan. Incident annex 5: Cyber annex.* Retrieved from https://vem.vermont.gov/sites/demhs/files/pdfs/plans/state/Incident%20Annex%205_Cyber%20Incident_2016_06.pdf

[80] Washington Military Department. (2015, March). *Washington state significant cyber incident annex to the Washington State Comprehensive Emergency Management Plan. Annex D.* Retrieved from https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf

[81] West Virginia Department of Homeland Security and Emergency Management. (2016, January). *Emergency Operations Plan. Incident specific annex 3: Cyber incident response.* Retrieved from http://dhsem.wv.gov/Resources/Documents/WV%20EOP%202016/IS%2003%20-%20Cyber%20FINAL%201-6-16.pdf

[82] State of Wisconsin Department of Military Affairs, Wisconsin Emergency Management. (2017, November). *Wisconsin Emergency Response Plan: Emergency Support Functions & Incident Specific Annexes.* Retrieved from https://dma.wi.gov/DMA/divisions/wem/preparedness/2017_WERP(Full37M).pdf

[83] Arizona Department of Emergency and Military Affairs. (2017, February 8). *Arizona State Emergency Response and Recovery Plan.* Retrieved from https://dema.az.gov/sites/default/files/publications/EM-PLN_SERRP_2017_FINAL_Feb08_2017.pdf

[84] Colorado Division of Homeland Security & Emergency Management. (2016, November). *Colorado Hazard and Incident Response and Recovery Plan.* Retrieved from https://www.colorado.gov/pacific/dhsem/state-eop

[85] State of Connecticut. (2018, August). *Cyber Disruption Response Plan.* Retrieved from https://portal.ct.gov/-/media/DEMHS/_docs/Cyber-Disruption-Response-Plan-Signed-Oct-2018.pdf?la=en

[86] State of Illinois. (2017, March 31). *Illinois Emergency Operations Plan: Annex 22—Information and cybersecurity.* Retrieved from https://www2.illinois.gov/iema/Preparedness/Documents/IEOP/Annex22.pdf

[87] State of Maine. (2016, May 26). *Emergency Operations Plan—Incident annex 3: Cyber incident.* Retrieved from http://www.maine.gov/tools/whatsnew/attach.php?id=732508&an=1

[88] Maryland Emergency Management Agency. (2019, January). *Consequence Management Operations Plan.* Retrieved from https://mema.maryland.gov/Documents/Maryland_Consequence_Management_Operations_Plan%202.0_January%202019_FINAL%201.pdf

[89] Commonwealth of Massachusetts. (2019). *Comprehensive Emergency Management Plan.* Retrieved from https://www.mass.gov/lists/comprehensive-emergency-management-plan

[90] State of Michigan Executive Office. (2015, October 25). *Cyber Disruption Response Plan* (page 21). Retrieved from https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf

[91] Ohio Department of Administrative Services, Office of Information Technology. (2018, March). *Emergency Operations Plan. Emergency Support Function #2: Communications and information technology. Tab B—Cyber Incident Response Plan.* Retrieved from https://ema.ohio.gov/Documents/Ohio_EOP/EOP_Overview/ESF-2%20-%20Tab%20B%20-%20Cyber%20Incident%20Response%20Plan%20-%202018.pdf

[92] State of Oregon. (2015). *Emergency Operations Plan. Incident annex 10—Cyber security.* Retrieved from https://www.oregon.gov/oem/Documents/2015_OR_eop_ia_10_cyber.pdf

[93] South Carolina Emergency Management Division. (2018, July). *South Carolina Cyber Incident Consequence Management Plan. Appendix 16 to the South Carolina Emergency Operations Plan.* Retrieved from https://www.scemd.org/media/1367/appendix-16-sc-cyber-incident-consequence-managment-plan.pdf

[94] Vermont Emergency Management. (2016, May). *State of Vermont Emergency Operations Plan. Incident annex 5: Cyber annex.* Retrieved from https://vem.vermont.gov/sites/demhs/files/pdfs/plans/state/Incident%20Annex%205_Cyber%20Incident_2016_06.pdf

[95] Washington Military Department. (2015, March). *Washington state significant cyber incident annex to the Washington State Comprehensive Emergency Management Plan. Annex D.* Retrieved from https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf

[96] West Virginia Department of Homeland Security and Emergency Management. (2016, January). *Emergency Operations Plan. Incident specific annex 3: Cyber incident response.* Retrieved from http://dhsem.wv.gov/Resources/Documents/WV%20EOP%202016/IS%2003%20-%20Cyber%20FINAL%201-6-16.pdf

[97] State of Wisconsin Department of Military Affairs, Wisconsin Emergency Management. (2017, November). *Wisconsin Emergency Response Plan: Emergency Support Functions & incident specific annexes.* Retrieved from https://dma.wi.gov/DMA/divisions/wem/preparedness/2017_WERP(Full37M).pdf

[98] Arizona Department of Emergency and Military Affairs. (2017, February 8). *Arizona State Emergency Response and Recovery Plan.* Retrieved from https://dema.az.gov/sites/default/files/publications/EM-PLN_SERRP_2017_FINAL_Feb08_2017.pdf

[99] Colorado Division of Homeland Security & Emergency Management. (2016, November). *Colorado Hazard and Incident Response and Recovery Plan.* Retrieved from https://www.colorado.gov/pacific/dhsem/state-eop

[100] State of Connecticut. (2018, August). *Cyber Disruption Response Plan.* Retrieved from https://portal.ct.gov/-/media/DEMHS/_docs/Cyber-Disruption-Response-Plan-Signed-Oct-2018.pdf?la=en

[101] State of Illinois. (2017, March 31). *Illinois Emergency Operations Plan: Annex 22—Information and cybersecurity.* Retrieved from https://www2.illinois.gov/iema/Preparedness/Documents/IEOP/Annex22.pdf

[102] State of Maine. (2016, May 26). *Emergency Operations Plan—Incident annex 3: Cyber incident.* Retrieved from http://www.maine.gov/tools/whatsnew/attach.php?id=732508&an=1

[103] Maryland Emergency Management Agency. (2019, January). *Consequence Management Operations Plan.* Retrieved from https://mema.maryland.gov/Documents/Maryland_Consequence_Management_Operations_Plan%202.0_January%202019_FINAL%201.pdf

[104] Commonwealth of Massachusetts. (2019). *Comprehensive Emergency Management Plan.* Retrieved from https://www.mass.gov/lists/comprehensive-emergency-management-plan

[105] State of Michigan Executive Office. (2015, October 25). *Cyber Disruption Response Plan* (page 21). Retrieved from https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf

[106] Ohio Department of Administrative Services, Office of Information Technology. (2018, March). *Emergency Operations Plan. Emergency Support Function #2: Communications and information technology. Tab B—Cyber Incident Response Plan.* Retrieved from https://ema.ohio.gov/Documents/Ohio_EOP/EOP_Overview/ESF-2%20-%20Tab%20B%20-%20Cyber%20Incident%20Response%20Plan%20-%202018.pdf

[107] State of Oregon. (2015). *Emergency Operations Plan. Incident annex 10—Cyber security.* Retrieved from https://www.oregon.gov/oem/Documents/2015_OR_eop_ia_10_cyber.pdf

[108] South Carolina Emergency Management Division. (2018, July). *South Carolina Cyber Incident Consequence Management Plan. Appendix 16 to the South Carolina Emergency Operations Plan.* Retrieved from https://www.scemd.org/media/1367/appendix-16-sc-cyber-incident-consequence-managment-plan.pdf

[109] Vermont Emergency Management. (2016, May). *State of Vermont Emergency Operations Plan. Incident annex 5: Cyber annex.* Retrieved from https://vem.vermont.gov/sites/demhs/files/pdfs/plans/state/Incident%20Annex%205_Cyber%20Incident_2016_06.pdf

[110] Washington Military Department. (2015, March). *Washington state significant cyber incident annex to the Washington State Comprehensive Emergency Management Plan. Annex D.* Retrieved from https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf

[111] West Virginia Department of Homeland Security and Emergency Management. (2016, January). *Emergency Operations Plan. Incident specific annex 3: Cyber incident response.* Retrieved from http://dhsem.wv.gov/Resources/Documents/WV%20EOP%202016/IS%2003%20-%20Cyber%20FINAL%201-6-16.pdf

[112] State of Wisconsin Department of Military Affairs, Wisconsin Emergency Management. (2017, November). *Wisconsin Emergency Response Plan: Emergency Support Functions & incident specific annexes.* Retrieved from https://dma.wi.gov/DMA/divisions/wem/preparedness/2017_WERP(Full37M).pdf