Meet the Threat: States Confront the Cyber Challenge
2016-17 NGA Chair's Initiative

Memo on State Cybersecurity Response Plans

General Overview

This memo identifies commonalities and differences among 32 cybersecurity incident and disruption response plans within 26 states. A cyber incident typically refers to data breaches, stolen personal identifiable information, unauthorized data encryption or any incident that affects data, which the state chief information security officer (CISO) has the authority to address.[1] A cyber disruption is an event, either man-made or natural, that temporarily disables critical infrastructure resources, such as electricity, finances and water.[2] Within the response plans, states defined "cyber events" to detail when and how they would prepare, respond and recover from a cyber incident or disruption event.

Among the 32 plans, 17 are incident response plans, 13 are disruption response plans and two are planning documents for establishing a response plan.[3] A majority of these plans are either a procedural document within the state's information technology (IT) agency or an annex to the statewide emergency operations plan (EOP) (See Table 1). Most states identified their IT agency as the lead agency for implementing the plan, while other states designated the homeland security departments, departments of public safety, or emergency management agencies, as the lead agencies (See Table 1).

Plans written as an annex to the state EOP or as a disruption response plan tended to identify more supporting agencies to assist in preparing, responding and recovering from a cyber event compared to those written as an IT policy. These plans embodied a whole of government approach by identifying fusion centers, state police, departments of military affairs, the National Guard, departments of public safety and others, to prepare and respond to a cyber event (See Table 1). To coordinate a state response among these actors, 19 states stand up a response team, the state emergency operations center, or a unified command structure (UCS) during a cyber event. **Virginia's** UCS, for example, has three lead agencies, with their IT agency managing cyber response activities, and their emergency management agency and state police coordinating response and recovery efforts. **Michigan** took a unique approach by centralizing all the relevant entities into one unit, the Cyber Disruption Response Team, with the IT agency acting as chairman and the Emergency and Homeland Security Division acting as vice chair.

Most plans divide roles and responsibilities among participating agencies by preparation, response and recovery activities. In roughly half of the plans, these roles are further broken down by specific threat levels. Although states differ in their lead agency's degree of involvement during these phases of a cyber event, there were some commonalities. During the preparation phase, lead agencies conduct risk assessments for state agencies, assist in agency network security, hold user awareness and response plan exercise, and assist state agencies develop communication protocols. More similarities were seen in response activities, which included assigning attribution, investigating the event, quarantining the event and prioritizing response efforts. The recovery phase tended to be a continuation of the response phase, but with an emphasis on investigating the incident, restoring less critical systems and conducting after-action reports.

Best Practices

Regardless of their size, population, economy or assets, every state is vulnerable to a cyber event that adversely affects citizens' private data or access to public services. Therefore, every state needs a comprehensive response plan with threat levels that are activated during significant cyber events. Combining the responses to cyber

[1] "Cyber Disruption Response Planning Guide," *National Association of State Chief Information Officers,* April 2016.
[2] *Ibid.*
[3] There are a few response plans that are called "Incident Response Plans," but define a cyber event as a cyber disruption.

incidents and disruptions will facilitate lessons learned across state agencies, reinforce relationships and institutionalize reactions to these events.

States should consider two approaches when creating a comprehensive response plan. The first option is for states to implement a response plan within their EOP, which has three benefits. The plan would call for activating specific emergency support functions (ESFs)—such as communications, emergency management and resource and logistics support—which avoids duplicating or contradicting existing plans. Moreover, state agencies are experienced at executing existing ESF responsibilities, which would assist in response efforts to a cyber event due to agencies familiarity with the ESFs. A second benefit is an activation of an EOP that activates the states emergency operations center (SEOC) or a unified command system, which then coordinates activities across all relevant parties. States should take advantage of their SEOCs experience in coordinating incidents and rely on their institutional knowledge to coordinate a response to a cyber event. Further, coordinating a response through a SEOC reinforces the necessity of a cyber event requiring a whole of government response to a cyber event. In summation, these plans recognize a cyber event's potential to transition from a technological consequence to a physical consequence and, as a result, ensures that all appropriate state agencies are ready to respond.

The second approach a state can undertake is similar to that of **Wisconsin**: create a cyber disruption strategy that identifies goals and objectives that must be met prior to implementing a plan. Wisconsin's plan identifies five core goals to create a response plan: (1) establish a cyber disruption governance authority; (2) identify organizations, roles, and processes; (3) develop risk profiles and capacities of state agencies and critical infrastructure; (4) improve communications across partners; and (5) develop and practice response and recovery operations. Every state, regardless of the approach they utilize to implement their plan, should detail these five core activities in their preparation phase. Heavily emphasizing the preparation phase of the response plan mitigates the impact of a potential cyber event and lessens the burden of the response and recovery phase.

States should consider their own needs, resources and capacities when developing response plans. However, response plans' effectiveness will be limited without a governance body or an agency that has the authority to adequately prepare the state to meet the threat. Response plans' lead bodies and agencies rely on employees who maintain good cyber hygiene to prevent intrusions, laws enabling prosecution of cyber criminals and strong relationships with critical infrastructure partners to facilitate a coordinated response to an event. Additionally, these plans' effectiveness are contingent upon the future pool of cybersecurity employees who are capable of implementing the plans. Therefore, states should contemplate creating a governance body, or increasing a relevant state agency's authority, that is responsible for implementing a response plan, and eventually expanding their scope to implement the statewide cybersecurity strategy. Centralizing statewide cybersecurity authority within a body or an agency allows that leader to tailor employee cyber hygiene programs, recommend key legislation, foster important relationships and recognize the specific workforce needs of the state. As a result, that cyber leader will have the tools in place to adequately prepare for an event, and have the human capital and relationships in place to adequately respond to a significant cyber event.

Table 1: Characteristics of State Response Plans

Question	Characteristics	Frequency
What type of plan is it?	Incident Response Plan	17
	Disruption Response Plan	13
	Planning Document	2
How was the plan written?	Annex to State Emergency Operations Plan	15
	IT Procedure	14
	Stand Alone	3
Who is responsible for implementing the plan?	IT Agency	20
	Emergency Management Agency	4
	Homeland Security Agency	4
	Department of Public Safety	2
	Cyber Disruption Team	1
	State Emergency Operations Center	1
What are the supporting agencies? (Agencies listed only include those that were mentioned at least twice)	Fusion Center	7
	State Police	7
	IT Agency	6
	Military Affairs	6
	Emergency Management Agency	6
	Department of Public Safety	6
	National Guard	5
	Attorney General's Office	4
	Governor's Office	4
	Homeland Security Agency	4
	Department of Administrative Services	3
	Higher Education	3
	Computer Crimes Unit/Bureau of Investigation	2
	Legal Counsel/Criminal Justice	2
	Public Utilities Commission	2
Does the plan activate a unified command system?	Cyber Disruption Team/Incident Response Team	10
	Unified Command Structure	5
	State Emergency Operations Center	3
	Cyber Response Assessment Board	1
	No	13
Does the plan have threat levels?	Yes	15
	No	16

***Alabama Cyber Security Incident Response* (DOC 2)**
Established: Created as an information technology procedure.

Purpose: The incident response ensures the state is prepared to respond to cyber security incidents, to protect state systems and data and prevent disruption of government services by providing the required controls for incident handling, reporting and monitoring, as well as incident response training, testing and assistance.

Lead Agency and Responsibilities: The information services division (ISD) provides incident response support resources that offer advice and assistance with handling and reporting of security incidents for users of ISD information systems. Additionally, ISD creates a cyber security incident response team (CSIRT) to ensure appropriate responses to cyber security incidents.

Incident Precursors and Responses: Identifies eight types of incident precursors and details responses to those precursors.

Incident Response Protocol: The response protocol includes preparation activities; detection and analysis activities; containment, eradication and recovery activities; and post-incident recovery activities.

- *Preparation*: Conduct risk assessments; harden host security; strengthen network security and malware prevention; and improve user awareness and training;
- *Detection and Analysis*: Determine whether an incident occurred; analyze the precursors and indicators; conduct research; document for investigative purposes; prioritize the incident response based on functional impact, information impact, and recoverability effort; and notify appropriate internal and external personnel;
- *Containment, Eradication, and Recovery*: Contain the incident; eradicate the incident by removing malware and mitigating all vulnerabilities that were exploited; and recover from the incident by returning affected systems to an operational state and confirming that affected systems are operating normally; and
- *Post-Incident Recovery*: Create a follow-up report and hold a lessons learned meeting.

Arizona Incident Response Planning 2015
Established: Created as a statewide policy.

Purpose: The incident response increases the ability of the budget unit (BU) to rapidly detect incidents, minimize any loss due to destruction, mitigate the weaknesses that were exploited and restore computing services.

Lead Agency: State chief information officer.

Supporting Agencies/Actors: CISO, state chief privacy officer; BU director; BU CIO; BU information security officer (ISO); BU privacy officer; supervisors of state employees and contractors.

Incident Response Protocol
Preparation:

- Incident Response Training: The BU shall provide incident response training to state information system users consistent with assigned roles and responsibilities before authorizing access to the state information system or performing assigned duties;
- Incident Response Testing: The BU shall test the incident response capability for the state information system annually using checklists, walk-through, tabletop exercises, simulations or comprehensive exercises to determine the incident response effectiveness and document the results;
- Incident Handling: The BU shall implement an incident handling capability for security incidents that includes:

    - Preparation, detection and analysis, containment, eradication and recovery
    - Incident handling activities with contingency planning activities
    - Incident response procedures, training and testing/exercises covering lessons learned from ongoing incident handling activities
    - Industry developments
    - Implementation of industry development changes where applicable;
- Automated Incident Handling Processes: The BU shall employ automated mechanisms to support the incident handling process;
- Assign Incident Handling Role: The BU shall assign to an individual or team the information security management responsibility of implementing an incident response plan and to be prepared to respond immediately to a system breach;
- Develop an incident response plan;
- Develop an automated support for availability of information; and
- Develop a privacy incident response plan.

Response:

- Incident Reporting: The BU shall require personnel to report Suspected security incidents to the organizational incident response capability within one hour of knowledge of suspected incident; and
- Automated Incident Reporting: The BU shall employ automated mechanisms to assist in the reporting of security incidents.

Arizona Cyber Incident Annex to EOP (2013)
Established: Cyber incident annex to state EOP.

Purpose: The cyber incident annex discusses policies, organization, actions and responsibilities for a coordinated, multidisciplinary, broad based approach to prepare for, respond to and recover from cyber-related incidents of statewide and/or national significance impacting critical state processes and economy.

Primary Agencies and Responsibilities: Department of homeland security and IT agency. The annex coordinators are the department of emergency and military affairs and the division of emergency management. Responsibilities include: serving as a computer support agency and security consultant; identifying performance measures for the operation of secure information systems; developing and implementing a statewide plan for IT; and ensuring state security architecture tech meets industry standards.

Supporting State Agencies: Department of administration, department of public safety, department of emergency and military affairs, division of emergency management, attorney general's office, computer crime unit, office of the governor and state universities. Responsibilities are on p. 621.

Threat Levels (Actions not included in this memo):

- *Green:* Probing of the network and servers is minimal and low risk viruses are contained thus not interfering with daily operations;
- *Blue:* Increased hacking and virus activity is detected. Potential malicious cyber activities and exploits may be identified but pose no significant impact on network and business functions;
- *Yellow:* Increased hacking, viruses and malicious activity are detected and pose the potential to compromise or diminish systems. Vulnerabilities are being exploited with moderate level damage or disruption;
- *Orange:* Indications of core critical infrastructure intrusions and malicious cyber activity are detected. Hacking, viruses and other significant malicious activity intrusions result in service outages, system compromises and critical infrastructure system failures; and

- *Red:* Widespread outages and/or significant destructive compromises to critical infrastructure debilitate systems.

Incident Response Protocol:
- ADEM determines the level of the incident and makes the recommendation to declare a state of emergency to the governor;
- Annex is activated;
- State will use its standard ESF program to meet any of the requirements generated by incident(s) of this nature and will support local and tribal jurisdictions in meeting the same priorities; and
- During recovery, ADEM may maintain activation of the SEOC to continue support operations and coordination of state/federal agencies response assets and resources.

Arkansas Cyber Incident Support Annex (2015)
Established: Created as an annex to the state emergency operations plan and based on NIMS.

Purpose*:* The cyber incident support annex discusses policies, organizations, actions and responsibilities for a coordinated approach to prepare for, respond to and recover from cyber related incidents impacting critical state government and educational processes.

Lead Agency and Responsibilities: The department of information systems (DIS) provides threat indications and warnings; provides training to agencies on conducting exercises; reports cyber incidents; maintains information sharing practices; analyzes cyber-attacks; assists law enforcement with cyber related investigations; attribute attack sources; and removes known sources of attacks.

Supporting Agencies and Responsibilities: The office of the governor ensures that critical government services remain available and keeps citizens aware of recovery efforts. The department of emergency management works with DIS to lead table top cybersecurity exercises and activates the emergency operations center to coordinate response and recovery efforts.

Colorado Cyber Incident Annex (Not Publicly Available)

Idaho Cybersecurity Annex (2015)
Established: An incident annex to the state's EOP.

Purpose: Provides guidance for a coordinated response by state, county, and federal agencies to significant events affecting the confidentiality, integrity, or availability of information technologies.

Lead Agency and Responsibilities: The department of administration, as the agency responsible for implementation of the cyber annex, will coordinate efforts with the IDEOC. They both may assign lead coordinating responsibilities to the appropriate agencies based on the impact of a cybersecurity incident. Responsibilities include:
- Coordinating and/or initiating alert/notification procedures and state response to requests for assistance from agencies;
- Maintaining situational awareness;
- Maintaining communications with federal agencies, governor's office and other state agencies;
- Ensure coordinated production of technical data;
- Provide technical liaison to the affected agency; and
- Support the flow of information.

Supporting State Agencies: Military division, bureau of homeland security, department of health and welfare, transportation department, tax commission, state controller's office, department of labor, state fusion center and state police. Responsibilities of these agencies are on p. 442 of the plan.

Threat Levels:

- *Low*: Malware events against state resources;
- *Guarded*: Website defacements, minor impact to state resources;
- *Elevated:* Impacting sensitive resources, web site compromise, impact to the confidentiality or integrity of sensitive information;
- *High*: Event impacting multiple agencies, risk to confidentiality that could pose a major impact to the state or individuals, impact to core infrastructure; and
- *Severe*: Impacting life safety, could affect power, ability of agencies to continue operations.

Kansas Incident Response
Established: Created as an information security policy.

Purpose: The incident response maintains availability, integrity and confidentiality and to document, authorize and establish continuing incident handling management standard disciplines and processes across the enterprise.

Incident Definition: A violation or imminent threat of violation of computer security policies, acceptable use or standard computer security practices. It is also any adverse event whereby some aspect of a computer system is compromised, such as loss of data confidentiality, disruption of data integrity, disruption or denial of service.

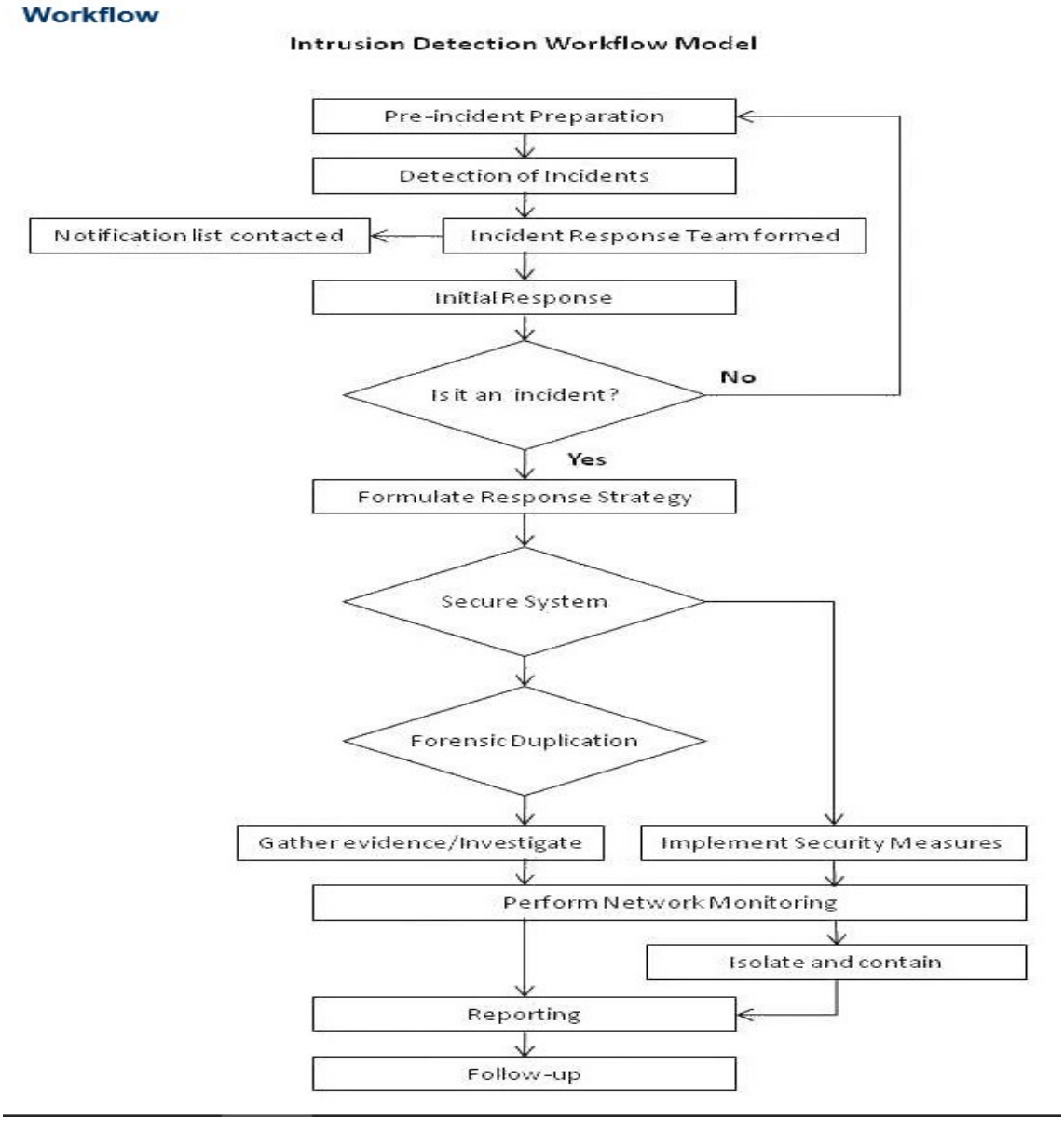
Incident Response Protocol:
Preparation:

- Each agency should appoint an official security point of contact (POC) and a secondary POC to act as a liaison with the state chief information security officer. When the security officer discovers a security incident occurring in an agency, he or she will report the incident to the agency POCs.

Response:

- Types of announcements include: "heads-up," alerts, advisories, for your information and guidelines;
- Upon learning of or suspecting a cyber incident, agencies are required to report information to the information security office; and
- See Figure 1 below for workflow model.

Figure 1: Kansas' Workflow Model



Kentucky Incident Response Plan (2015)

Established: Within the office of technology as a policy, created in 2013 and revised in 2015.

Purpose: The incident response plan identifies the necessity and procedures for agencies and COT to identify and notify appropriate personnel when a security incident occurs.

Definition of Cyber Incident: An information security incident, as defined in national institute of standards and technology (NIST) special publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies or standard security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the exploited weaknesses and restoring computing services.

Primary Agency: Office of the CISO.

Incident Response Protocol

- When agencies identify a potential security incident, they are required to contact the commonwealth service desk to report the incident;
- The office of the CISO will review all incidents and, on a case-by-case basis, determine whether to become actively involved depending on the actual or potential expansion of the incident to other assets or agencies; and
- Five phases of security incident handling:
    - Notification, Assessment, and Initial Response
    - Evidence Gathering
    - Remediation
    - Incident Assessment and Reporting
    - Post-incident Activities, to include Lessons Learned.

Louisiana Incident Response Plan

Establish: An appendix to the state's information security policy.

Purpose: The incident response plan clearly outlines the required actions and procedures required for the identification, response, remediation and follow-up to incidents, with the intent of responding appropriately and in a timely manner to all security events and incidents.

Definition of Incident: The CISO or designee within the information security team (IST) will determine if the security event justifies a formal incident response.

Primary Agency: The CISO and incident response team (IRT) will begin the formal incident management process starting with assigning an appropriate classification level to the incident.

Supporting Personnel: The following make up the IRT: the CIO; CISO; additional IT personnel; subject matter experts in legal and compliance, public communications, HR and information security; an agency relations manager that is appointed by the office of technology services for each state agency; and others.

Threat Levels: The CISO or designee within the information security team (IST) will determine if the security event justifies a formal incident response. Classifications are determined by evaluating the likelihood and potential impact of an incident. There are four levels:

- *Low:* One instance of potentially unfriendly activity (e.g., port scan, malware detection, unexpected performance peak, observation of potentially malicious user activity, theft of a device, etc.).
- *Medium:* One instance of a clear attempt to obtain unauthorized information or access or a repeated or persistent low incident. Incidents classified as medium risk may also include the incidental internal exposure of one employee record. Medium incidents may also include vulnerabilities with a rare rate of occurrence on critical systems.
- *High:* Serious attempt or actual interruption in availability, or negative impact to confidently or integrity, or data breach or a repeated or persistent Medium Incident. Incidents with a high criticality may include systems with low to moderate criticalities which are affected by vulnerabilities likely to be exploited.

- *Emergency:* Incidents that involve the potential breach of restricted or confidential data. Incidents with an emergency criticality are likely to be assets with high criticality to business functionality which are affected by threats which are almost certain to occur.

Incident Response Protocol: Each personnel and group is assigned roles and responsibilities. Below is general overview of the incident response:

- *Communications:*
  - Internal Notifications
  - External Notifications
  - Breach Notifications
- *Investigation and Evidence Collection*
- *Containment:*
  - Short-Term
  - Long-Term
- *Root Cause Analysis*
- *Eradication*
- *Recovery and Remediation*
- *Lessons Learned*
- *Continuous Evaluation:*
  - Training: All state employees, contractors, consultants, temporary employees, and other staff members, receive security awareness training upon hire and annually thereafter that includes their responsibilities in notifying the CISO, or designee when they become aware or observe a security event; and
  - Testing: The incident response plan must be organized by the CISO to be tested at least every 12 months' basis without prior notification.

Maine Major Incident Procedure 2014

Establish: A procedure document within the office of information technology (OIT).

Purpose: The major incident procedure utilizes a pre-defined procedure, agencies and OIT to collectively ensure the best possible response to major incidents and applies to executive branch agencies and other state government branch applications hosted by OIT.

Definition of a Major Incident: Event judged to have a significant impact on governmental information operations.

Primary Agency: CIO owns, executes and enforces this procedure, communicates to commissioners, determines and declares a disaster.

Supporting Agencies and Responsibilities:

- Chief technology officer (CTO), associate CIO applications, TBC director or their designees determines and declares a major incident;
- Communications coordinator coordinates all internal and external major incident communication. Works closely with the TBCs to keep all parties informed. Provides accurate and timely updates to the customer support status (CSS) page;
- Duty manager facilitates initial remediation for any incidents and IT outages during off-business hours and reports potential major incidents to the CTO, associate CIO applications, or TBC director;
- Enterprise security officer serves as incident response team leader for cybersecurity incidents. Has the authority to declare a major incident for any imminent cybersecurity threat;
- Incident response team responds to a major incident;

- Incident response team leader owns, manages, and leads major incident response. forms and manages the incident response team, serves as, or designates, the communications coordinator; and
- Technology business consultants (TBCs) communicates or acts as a liaison to key agency personnel during the major incident. Disseminates official communication received from the communications coordinator.

Incident Response Protocol:

Awareness and Initiation

- Any OIT employee that becomes aware of a potential major incident immediately notifies their management. If the manager/director does not have the authority to determine and declare a major incident, they report the potential major incident to the CTO, associate CIO applications, or TBC director;
- The CTO, associate CIO applications, TBC director or their designee determines if it is a major incident. If so, they designate the incident response team leader and initiate major incident response. if not, they assure the initial reporter that it is a routine matter and routine response or remediation is undertaken;
- The CTO, associate CIO applications, or TBC director informs the CIO of any major incident they believe may have reached disaster level;
- If the CIO determines the major incident has indeed reached a disaster level, disaster recovery response is initiated in accordance with pertinent OIT business continuity/disaster recovery plans; and
- The enterprise security officer has the authority to declare a major incident, and initiate the major incident response for any cybersecurity incident

Response

- The incident response team leader (IRTL) forms the incident response team and identifies the communications coordinator. The IRTL must also consider whether the OIT emergency operations center should be activated to help facilitate remediation;
- IRTL consults with the incident response team to confirm the remediation strategy, including recovery time objectives (RTO) and recovery point objectives (RPO);
- IRT initiates remediation steps, including any required coordination with other OIT resources, vendors, suppliers, partners, etc.;
- The communications coordinator communicates with TBCs and other OIT personnel as required to facilitate information flow and official message content; and
- The communications coordinator updates OIT customer support. OIT customer support posts updates to the CSS page. This is minimally once per hour until remediation.

Diagnosis and Remediation

- IRT diagnoses the cause and estimates remediation time;
- IRT continuously updates the communications coordinator;
- IRTL ensures that a service ticket is created for the major incident; and
- IRT performs required remediation.

Post-Remediation

- IRT documents the service ticket(s), ensures service tickets are created for any follow-up activities, and that all service tickets are linked;
- Upon resolution, the IRTL creates a preliminary report (approved by the CIO prior to distribution), which is distributed to impacted customers (by the TBCs) within two business days; and
- IRTL creates an OIT major incident report (approved by the CIO prior to distribution), which is distributed to all concerned parties (by the TBCs) within five business days of resolution. The report includes full details of the incident and root cause analysis.

Massachusetts Enterprise Security Incident Response Policy (2014)

Established: Policy within the department of administration and finance.

Purpose: The incident response policy articulates the requirements for responding to security incidents and attack intrusions.

Definition of Cyber Incident: Security incidents include cyber stalking, child pornography, unauthorized disclosure of IT systems and data, web page defacement, disclosure of passwords, harassment and threats conducted via email, DDOS attacks casing system crashes, and changes to hardware and software.

Policy Application: All secretariats and their respective agencies and entities governed by the overarching enterprise information security policy must adhere to the requirements of this supporting policy.

Agencies that enforce the plan: Assistant secretary for IT, secretariat CIO and agency head, agency ISO, enterprise security board, and information technology division,

Agencies Responsibilities:

- Report security incidents affecting executive department agencies;
- Contact the governor's chief legal counsel about security incidents that may constitute criminal conduct;
- Notify the information technology division;
- Designate IT personnel who have the authority to make the immediate technical and managerial decisions; and
- Proactively establish authorization procedures for expenditures associated with incident remediation that do not unreasonably impede IT staff from addressing a situation.

Michigan Cyber Disruption Response Plan (2015)
Establish: Part of Gov. Rick Snyder's Cyber Initiative, which was launched in 2011.

Purpose: The cyber disruption response plan (CDRP) provides emergency management, IT, and other potential stakeholders, within Michigan, a management framework to coordinate preparedness, response, and recovery activities related to a large-scale or long-duration cyber disruption. The CDRP also consists of a communication annex, a cyber response plan template for critical infrastructure, a training and exercise annex, and a risk management framework annex.

Lead Agency: The cyber disruption response team (CDRT) is the coordinating structure for cyber disruption incidents. CDRT's leadership is composed of representatives from the department of technology, management and budget (DTMB) and the state police. The chief security officer (CSO) acts as the CDRT chairman and the deputy director of emergency management and homeland security division (EMHSD) serves as the vice chairman. The CDRT internal structure follows NIMS/ICS principles.

Supporting Agencies: CDRT's core group contains state members from DTMB (this includes the Michigan information sharing and analysis center), EMHSD, Michigan Cyber Command, intelligence operations center, National Guard, private sector entities and others as determined necessary. Regional and national contacts are within CDRT as well.

Threat Levels: Michigan has a cybersecurity threat matrix that details five threat levels. For each threat level, CDRP details the level definition, threat escalation/de-escalation criteria, potential impact, communication procedures and agencies' responsibilities.

Incident Response Protocol: The CDRT is responsible for the following three phases and activities:

- *Preparation*: Identify threats and vulnerabilities to IT networks; identify mitigations for threats and vulnerabilities; develop communication means; develop plans to address specific disruptions; and train and exercise this plan.

- *Response*: Monitor disruption events to determine scale/scope and if event is stable or worsening; share information with and assist other CDRTs; help coordinate IT-related response activities; and assist incident/unified command staff.
- *Recovery*: Determine resources needed to restore affected systems; track restoration efforts; work with emergency management recovery leads; and conduct internal and external CDRT after-action reviews.

Minnesota Enterprise Security Incident Management Guide 2013

Mississippi Cyber Incident Annex (2012)
Established: Created as an annex to the emergency management plan.

Purpose: The cyber incident annex outlines policies, organizations, actions and responsibilities for a coordinated, multidisciplinary, broad-based approach to prepare for, respond to and recover from cyber-related incidents impacting critical Mississippi processes and economy.

Lead Agency and Responsibilities: The information technology systems (ITS) provides indications/warnings of potential cyber incidents; engages in information sharing; analyzes cyber vulnerabilities; provides technical assistance; assists in criminal investigations; attributes the source of cyberattacks; and leads state recovery efforts.

Supporting Agencies: The department of homeland security; emergency management agency; department of public safety; and other agencies as deemed appropriate will provide supporting functions.

Montana Information Security Advisory Council Best Practices Working Group-Large Cyber Incident Handling (2016)
Established: A document created by the council's best practices working group in 2016.

Purpose: The document provides technical best practices on dealing with a high or critical cyber incident.

Incident Response Protocol:
Preparation
- Each agency must develop and document an information systems incident response team (ISIRT) and be prepared to handle incidents; and
- Agencies will use those tram's templates provided as a model in developing an incident handling plan within their organization.

Detection & Analysis Phase
- Actions performed on the information system should cease;
- Activate ISIRT once incident is confirmed to be real;
- Review of SIEM data, packet captures (PCAP), automated detection logs, 3rd party information, IDS/IPS logs, etc. should be performed verifying validity and scope of the incident; and
- The IC will continue documenting important events, with timestamps, as they unfold until a delegated authority is assigned to take over this duty.

Containment Phase
- Plan details several actions to take depending on the breach and the systems that are breached.

Eradication Phase:
- After containment, eradication should be performed to eliminate components of the incident. Identifying all affected hosts within the organization is critical so they can be remediated;
- Actions such as deleting malware, disabling breached user accounts, identifying and mitigating vulnerabilities, or complete rebuild of the information systems should be performed if approved by management; and
- Deactivation of the organizations ISIRT can be performed at this time and conduct AAR.

Recovery Phase

- Start restoring from clean backups, rebuilding systems, installing patches, changing passwords, and tightening network security;
- Higher level of system logging and/or network monitoring should be considered on all systems within an organization due to the increased chance of system(s) being attacked again; and
- Confirmation systems are functioning normally and vulnerabilities are remediated should be performed to prevent similar incidents.

Post-Incident Activity

- Documentation created during the incident should be used to prepare a post incident report. This report should include items such as cause, plan of actions and milestones (POA&M) or gap analysis, lessons learned, cost, need for evidence retention, recommendations for immediate action, and long term goals to prevent another similar incident; and
- Information sharing to the security threat group.

New Hampshire Catastrophic Cyber Disruption Plan (Not Publicly Available)

New York Cyber Incident Response (2015)

Established: Created as an independent standard by the New York State Information Technology Standard (ITS).

Purpose: The incident response outlines the general steps for responding to computer security incidents. In addition to providing a standardized process flow, it (1) identifies the New York State (NYS) incident response (IR) stakeholders and establishes their roles and responsibilities; (2) describes incident triggering sources, incident types, and incident severity levels; and (3) includes requirements for annual testing, post-incident lessons-learned activities, and collection of IR metrics for use in gauging IR effectiveness.

Lead Agency and Responsibilities: The state CISO, who leads the enterprise information security office (EISO), provides overall coordination of the incident response.

Supporting Agencies and Responsibilities: The EISO cyber incident response team (CIRT) responds to incidents by providing hands on technical incident response and recommend steps for agencies to remediate and mitigate attacks. The EISO cybersecurity operations center serves as a central group for collaboration and information sharing with other entities that may be experiencing the same or similar incidents, to help resolve the problem more quickly than if done separately. All state agencies must have predefined teams at the ready which include, at minimum, executive management, legal and the public information officer. The state's fusion center, state police, internet service providers and other private security industries may play a role as well.

Incident Categories/Severity Matrix: Adopted six US-CERT incident categories that include: exercise/network defense testing, unauthorized access, denial of service, malicious code, improper usage, scans/probes/attempted access, and investigation. Additionally, they have adopted a three-level, severity matrix that defines what is considered a high, medium, or low incident.

Incident Response Protocol: The plan has six steps: preparation, identification, containment, eradication, recovery and lessons learned.

Preparation: Activities include stablishing incident response (IR) teams; updating IR tools, policies/procedures, and forms/checklists; and ensuring IR communication procedures and IR stakeholder contact lists are accurate and up-to-date.

Identification: Involves review of anomalies to determine whether or not an incident has occurred, and, if one has occurred, determining the nature of the incident. Agencies must follow incident categories and severity matrix.

Containment: Information is collected to determine how the attack took place. All affected systems within the enterprise should be identified so that containment (and eradication and recovery) is effective and complete.

Eradication: Removing elements of the threat from the enterprise network. Specific eradication measures depend on the type of incident, number of systems involved and the types of operating systems and applications involved.

Recovery: Remediate any vulnerabilities contributing to the incident (and thus prevent future incidents) and recover by restoring operations to normal. Typical recovery activities include rebuilding systems from trusted images/gold standards, restoring systems from clean backups and replacing compromised files with clean versions.

- *Lessons Learned*: A record of steps taken to respond to an attack; investigative results into determining the root cause of the attack; and potential improvements to make, such as IR stakeholder training and certifications, process and procedural updates and technical modifications.

North Carolina Significant Cybersecurity Incident (2015) (Not Publicly Available)

North Carolina Cyber Security Incident Response in the Statewide Information Security Manual (2016)
Established: A chapter in the state's statewide information security manual and details several policies for different types of scenarios.

Purpose: The manual details specific policies for several scenarios, which include:

- Defending against cyber attacks;
- Defending against internal threats;
- Safeguarding against malicious denial of service attacks;
- Defending against hackers, stealth- and techno-vandalism; and
- Defending against malware attacks.

Plan composition: The plan is comprised of the following sections:

- Combating cyber crime and policies for the different crimes; and
- Reporting information security incidents

Threat Levels:

- *Low/Green*: Isolated instances of viruses and small number of system probes detected
- *Guarded/Blue*: External penetration or DDOS attempted with no impact;
- *Elevated/Orange*: significant level of network probes; widespread instances of a known computer virus; isolated instances of a new computer virus;
- *High/Yellow*: Penetration or DDOS detected with limited impact on NC state network operations; widespread instances of a new computer virus that cannot be handled by anti-virus software; small risk of negative financial or public relations impact*; and*
- *Severe/Red:* Successful penetration or DDOS detected with significant impact; significant risk of negative financial or public relations impact.

Oregon Cyber Incident Annex
Established: Created as an annex to the emergency management plan.

Purpose: The incident annex facilitates effective and coordinated state and local government response and recovery activities to cyber incidents; outlines policies, organizations, actions and responsibilities for a coordinated, multidisciplinary, broad-based approach to prepare for, respond to and recover from cyber-related incidents.

Lead Agency and Responsibilities: The department of administrative services (DAS)/enterprise security office coordinates a cyber response through a unified command structure based on NIMS. DAS also conducts situational and periodic readiness assessments, plans for short/long term incident management recovery operations; and analyzes cyber vulnerabilities.

Supporting Agencies' Responsibilities: DAS, military department, other impacted state agencies, law enforcement and technology resources from the private and public sector. Specifically, they are responsible for participating in planning for incident management and recovery operations; conducting situational assessments; and maintaining trained personnel to respond to an emergency response. The annex does mention the state's fusion center, but does not detail its responsibilities.

Threat/Activation Levels: The annex has three activation levels: standby, limited and full. Limited refers to an escalated localized emergency or when a city fails to act. Full activation occurs if the governor declares a state of emergency; when there is a known terrorist threat or attack occurs; or an alert from a nuclear plant. Procedures in this annex also become activated when determined necessary by DAS, the office of emergency management and the governor.

Incident Response Protocol: Once a cyber incident occurs, DAS establishes facts and assumptions; recommends the threat level; provides recommendations to impacted agencies; assesses the ongoing impacts of the incident; identifies requirements for consequence management; and prioritizes actions for the restoration of computer and network services.

Oregon Incident Response Plan

Established: Enterprise security office created the incident response plan in 2015. Adopts NIMS and the ICS methodology and was created in coordination with Office of Emergency Management.

Purpose: The incident response plan describes how resources are to be brought together to respond to an information security incident, and to facilitate quick and efficient responses to incidents.

Definition of Incident: A single or a series of unwanted or unexpected information security events that result in harm, or pose a significant threat of harm to information assets and require non-routine preventative or corrective action.

Primary Role "Incident Commander": The commander has overall responsibility for managing the incident by establishing objectives, planning strategies, and implementing tactics. The governor may be the commander for incidents level 3 or 4, while the CIO is the commander for levels 2, 3 or 4.

Supporting Agencies: DAS director, CISO, enterprise security office, enterprise technology services, office of emergency management, legal counsel and public information office

Creates a Security Incident Response Team

Threat Levels (Actions not detailed in this memo):

- *Event Triage:* Agency must determine whether the event is an incident that requires non-routine incident response activities;
- *Minor:* theft of a laptop, malware infection requiring non-routine mitigation activity;
- *Medium:* incidents having "hard cost" impacts, malware outbreaks that impact multiple workstations;
- *Major:* major business impacts; and
- *Critical:* highest level of impact to state systems or government, DOS attacks against major infrastructure, terrorist activity.

Escalation of the incidents occurs through triggers that include: publicity, scope change, responsibility change, resource constraints, political sensitivity or perceived or actual mismanagement.

Have a communications protocol

Incident Response Protocol:

- *Preparation*
- *Detection and Analysis:*
    - The ESO will assist agencies and other stakeholders in the process of incident identification and analysis if requested
- *Containment*
- *Eradication and Recovery*
- *Post-Incident Activity*

Pennsylvania IT Security Incident Reporting Policy (2012)
Established: Created as an information technology policy in 2012.

Purpose: The security incident reporting and escalation policy enables the enterprise to respond effectively to security incidents, by clearly detailing the roles and responsibilities of all the parties involved. It provides a precise path for reporting, escalating, auditing and remediating security incidents.

Definition of Security Incident: Any occurrence involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse, or access to information technology resources such as systems, files, and databases.

	Critical/High	Medium	Low	Unknown
Description /Criteria	-Agency has found an active attack on an agency system. -Agency has found that other organizations' systems are affected. -Agency has found that the resources involved are in the critical categories. -Agency has determined that the data involved is restricted.	-Agency found that the resources involved are medium. -Data involved is for internal use only. -Incident has an impact of a financial loss, loss of data, violation of regulation, damage to the integrity of critical goods. -Agency has been unable to resolve the incident.	-Resources involved are in the low category. -Data involved is classified. -Agency has contained or resolved the incident.	-Agency has not determined all of the resources involved. -Scope of the data involved is unknown. -Agency has yet to contain or resolve the incident.
Reporting Requirement	-Agency ISO is required to notify the PA-CSIRT within 30 minutes of detection	-Agency ISO is required to notify the PA-CSIRT within 30	-Agency ISO is required to notify the PA-CSIRT within	-Agency ISO is required to notify the

		minutes of detection	30 minutes of detection	PA-CSIRT within 30 minutes of detection
Incident Reporting Forms	-Agency ISO must fill out the Incident Reporting Form	-Agency ISO must fill out the Incident Reporting Form	-Agency ISO must fill out the Incident Reporting Form	-Agency ISO must fill out the Incident Reporting Form

South Carolina Information Security Incident Response

Established: Created by the department of administration as a standards and procedures document.

Purpose: The information security incident response provides standards and guidance for information security incident response to all state agencies.

Lead Agency: The security operations center (SOC) at the South Carolina Information Sharing and Analysis Center (SC-ISAC) will provide response measures recommendations.

Threat Levels: There are five threat levels with corresponding responses:

- *Tier-5:* Malicious code or software was detected on the machine, but was not fully compromised and no risk of sensitive information loss;
- *Tier*-4: affected machine is fully compromised; meaning that a malicious user has obtained unauthorized administrative control over the machine but there is no immediate risk of sensitive information loss;
- *Tier-3:* machine is fully compromised and there is a possibility that sensitive information could have been accessed or lost;
- *Tier*-2: affected machine is fully compromised and network traffic suggests that information has been lost; and
- *Tier*-1: a very serious incident of a criminal nature, usually brought to the attention of SOC through law enforcement agencies.

Incident Response Protocol: Protocol is based on a five tier response system that defines the threat/incident and recommended response:

- *Tier-5:* Agency IT personnel will use tools to attempt to clean the machine, place the machine back in service, and document the updated IP address;
- *Tier*-4: Agency IT personnel will wipe the hard drive and re-image in accordance with agency incident response procedures. Agency IT should not attempt to clean the machine. Any passwords used on this machine must be changed;
- *Tier*-3: Agency IT personnel will locate the affected machine, interrupt the user and determine if there is any access to sensitive information from the affected system;
- *Tier*-2: Agency IT personnel will locate the affected machine and interrupt the user; Agency security officer or designee will bring the hard drive and chain of custody form to SC-ISAC for analysis when requested or seek forensic analysis services from local law enforcement; and
- *Tier*-1: All response procedures will be handled by the appropriate law enforcement agency with SOC assistance.

Texas Cyber Hazard Annex Emergency Management (2013)

Established: Created as a hazard annex to supplement the emergency management plan.

Purpose: The cyber hazard annex emergency management defines the organization, operational concepts, responsibilities and procedures to accomplish a coordinated response to threats and incidents involving the information technology (IT) systems and assets of state and local government that have or may have widespread impacts on the state's critical infrastructure, or threaten public safety and well-being.

Lead Agency and Responsibilities: The executive director of the department of information resources (DIR) provides guidance and direction to the state chief information security officer. The DIR provides indications and warnings of potential threats; leads investigative efforts; analyzes cyber vulnerabilities; attributes the source of cyberattacks; defends against attacks; leads state-level recovery efforts; and completes after action reports. The DIR also created a CSIRT to improve the state's ability to prevent, detect, respond to, and recover rapidly after an incident that has a significant cyber impact.

Supporting Agencies and Responsibilities: The office of the attorney general (OAG), the department of public safety (DPS) and the state auditor's office play a supporting role during a cyber incident. Specifically, the OAG's computer forensics unit and cyber crimes unit provide investigative and prosecution assistance. Divisions within the DPS, such as the computer information technology and electronic crime program, the crime laboratory service and the intelligence and counterterrorism division, will assist in investigations. Other agencies and organizations that are not named are responsible for maintaining trained personnel to assist DIR; developing and maintaining an inventory of resources and contact lists; providing situational and operational situation reports; and providing additional emergency resources if needed.

Threat Level and Responses: Texas has four threat levels and prescribed responses based on the threat levels, which are based on NIMS:

- *Normal Conditions (no disruptions)*: The DIR reviews and updates operating procedures; trains personnel to ensure understanding of the cyber hazard annex; and updates agency resource information;
- *Increased Readiness Conditions (minor disruptions)*: The DIR reviews plans and procedures to ensure ability to meet anticipated challenges; identifies personnel/resources shortfalls; and updates contact lists;
- *Escalated Response Conditions (major disruptions to essential state services)*: The DIR determines communication requirements and provides situational and administrative reports; and
- *Emergency Conditions (governor emergency declaration)*: The DIR implements actions to accomplish mission assignments; creates situation report of mission assignments; and gathers and analyzes situation information and submit reports.

Vermont Cyber Annex in EOP (2016)
Established: Updated in 2016 as an incident annex to the EOP.

Purpose: The cyber annex in EOP creates an emergency action plan in response to a significant intrusion into the state or private sector cyber environments.

Lead Agencies: Department of information and innovation and division of emergency management and homeland security (DEMHS).

Supporting State Agencies: Vermont state police, criminal justice services-office of technology management, national guard and attorney general's office.

Definition of Significant Cyber Incident: An event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the economy or diminish the security posture.

Threat Levels:

- *None:* No effect to the organization's ability to provide all services to all users and no information was compromised;
- *Low:* Minimal effect; the organization can still provide al critical services; sensitive PII was accessed;
- *Medium:* Organization has lost the ability to provide a critical service to a subset of system users; unclassified proprietary information, such as PCII, was accessed; and
- *High:* Organization is no longer able to provide some critical services to any users; sensitive information was changed or deleted.

Incident Response Protocol:

- The Cyber response assessment board (CRAB) will coordinate the response to any significant cyber event affecting state or private sector technologies which meets thresholds of significance
    - CRAB consists of the DEMHS, the VT intelligence center, CISO, and National Guard;
- Each department and agency involved in a significant cyber incident shall be responsible for ensuring the availability of its representative to the CRAB;
- CRAB will provide guidance to leaders in the SEOC, if activated;
- CRAB will use the escalation and notification matrix;
- Each agency is responsible for developing and maintaining its own cyber monitoring and impact assessment procedures; and
- Each agencies' roles and responsibilities are detailed on p.6 of the document.

Vermont Incident Response Plan in the Department of Information and Innovation (2010)

Established: Created in 2010 by the department of information and innovation.

Purpose: The incident response plan establishes a protocol to guide a response to a computer incident or event impacting the state's computing equipment, data or networks.

Definition of Computer Security Incident: An act or circumstance in which there is a deviation from the requirements of security regulations. Compromise, inadvertent disclosure, need-to-know violation and administrative deviation are examples of security incidents, including any unauthorized activity that threatens the confidentiality, integrity or availability (CIA) of state information system resources.

Incident Response Protocol:

- *Incident Reporting:* All computer security incidents shall be reported to the agency IT manager or agency supervisor;
- *Escalation:* The agency IT manager needs to determine the criticality of the incident;
- *Mitigation and Containment:* Affected systems, such as those infected with malicious code or systems accessed by an intruder shall be isolated from the network until the extent of the damage can be assessed. Any discovered vulnerabilities in the network or system will be rectified by appropriate means as soon as possible;
- *Eradication and Restoration:* The extent of damage must be determined and course of action planned and communicated to the appropriate parties;
- *Information Dissemination:* The CIO and/or his/her designee shall manage the dissemination of incident information to other participants, such as law enforcement or other incident response agencies;
- *Ongoing Reporting:* AAR is written and submitted; and
- *Review:* After the initial reporting and/or notification, the IT manager, department/agency managers and CIO shall review and reassess the level of impact that the incident created.

Virginia Hazard-Specific Annex #8: Cyber Incident Response (Not Publicly Available)

Washington State Security Incident Communication (2014)
Established: An incident response plan within the Office of the Chief Information Officer.

Purpose: The incident communication ensures the scope and impact of IT security incidents are properly evaluated and that a coordinated, centralized approach is used to determine if, when and how to communicate notification of an incident.

Cyber Incident Definition: Any unplanned or suspected event that could pose a threat to the integrity, availability or confidentiality of an agency's, or the state's, data or systems.

Lead Agency: Chief information security officer.

Incident Response Protocol:

- Agencies shall report all IT security incidents to the CISO;
- State CISO and consolidated technology services (CTS) security operations center (SOC) shall investigate to determine degree of severity and assist with mitigation
    - Upon being notified by an agency, the CISO and/or his/her staff will promptly work with agency IT security staff and any identified external parties to determine the scope and severity of the incident
    - CISO will provide assistance to the agency to identify the cause of the incident and determine what corrective steps should be taken to eliminate any identified vulnerabilities
    - The CISO will:
        - Determine whether the impacts of the incident are confined to the single agency or may affect multiple agencies.
        - Work with law enforcement agencies if necessary to gather additional information and assists with their investigations.
        - Provide available tools to the agency to help analyze the current incident and prevent future occurrences;
- State CISO shall notify the state CIO (if required)
    - After analysis of the incident, the CISO, at his/her discretion, will notify the state CIO and the assistant attorney general for the office of the chief information officer (OCIO) to provide details on the nature, scope and possible impacts of the incident and provide recommendations on what, if any, further actions should be taken.
    - At this time the CISO, in conjunction with the Washington State Office of the attorney general, will also provide the state CIO with an informed opinion as to whether or not the severity of the incident's impact warrants public notification as required by law;
- State CIO will convene security incident communication team (SICT) (if required)
    - Should it be determined by the CIO that public notification of an IT security incident is required by law, the CIO, at his/her discretion, will promptly convene a security incident communication team
    - The state CIO will notify the governor's office that an incident has occurred and may require public disclosure; and
- State CIO will authorize and coordinate release of public notification with breached agency(s) (if required)
    - Agencies will fully cooperate with the governor's office in support of disclosure of the incident, and will coordinate with the CIO on any requests from the public for information related to the incident.

Washington State Significant Cyber Incident Annex (2015)
Established: Created in March 2015 as an annex to the state comprehensive

emergency management plan.

Purpose: The cyber incident annex establishes the strategic framework to prepare for, respond to, and begin to coordinate response to and recovery from a significant cyber incident. Additionally, it operates as a strategic and operational framework for coordination and execution among state, local, tribal, territorial and federal governments; the private sector; and operators of cyber critical infrastructure partners.

Cyber Incident Definition: An event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity or availability of electronic information, information systems, services or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the economy or diminish the security posture.

Lead Agency and Responsibilities: The state emergency operations center (SEOC), under the guidance of the cyber unified coordination group and homeland security advisor (HSA), monitors and coordinates the state's cyber response activities. This command structure and the incident response protocol are based on NIMS.

Supporting Agencies: The office of the chief information officer; consolidated technology services director; director of emergency management; chief information security officer; telecommunications and energy, affiliated tribes of northwest Indians; university of Washington's center for information assurance; private industry/critical infrastructure and key resources representatives from the 18 sectors; National Guard; state patrol high tech crimes unit; Washington Fusion Center; and the office of the governor.

Incident Response Protocol:

- *Pre-Incident activities*: SEOC collaborates with a wide range of departments, agencies, and organizations on a daily basis to share information and identify threats, vulnerabilities, and potential consequences;
- *Incident Response activities*: SEOC, under the guidance of the HSA, coordinates operational response activities including incident prioritization, critical resource allocation, and situational awareness for issues arising as a result of a significant cyber incident. Additionally, the SEOC ensures appropriate enterprise protection controls are deployed and provides information on the incident to partners and executive leadership; and
- *Supporting agencies' responses*: The Washington Fusion Center generates cyber alerts to notify state, regional, local, tribal, federal, and private sector partners with early warning indicators and potential actionable intelligence measures. The state patrol investigates cybercrimes committed on state property, against state agencies, and against state assets.

West Virginia Cyber Incident Response Annex to EOP (2016)
Established: Cyber incident response for EOP.

Purpose: The incident response annex discusses policies, organizational structure, actions and responsibilities for a coordinated, multidisciplinary, broad-based approach to prepare for, respond to and recover from cyber-related incidents impacting critical state processes and infrastructure.

Coordinating Agency: Division of homeland security and emergency management is responsible for the development and maintenance of this annex. This should occur at minimum once every two years.

Primary Supporting Agencies: Office of technology and the intelligence fusion center. (Responsibilities on p. 6).

Support Agencies and Organization: Department of military affairs and public safety.

Incident Response Protocol:

- *Pre-Incident:* State departments and agencies maintain computer incident response capabilities that can rapidly respond to cyber incidents on their networks, including events of prolonged duration;
- *Notification and Activation Procedures:* Procedures in this annex are implemented when it is determined that a cyber related incident is imminent or underway. Notification of WVDHSEM is made through established communications channels that exist between the state government, nongovernmental entities and the public; and
- *Initial Actions:* WVDHSEM, WVOT, and other State/Federal agencies as appropriate work closely together to coordinate the response during a cyber-incident or attack, identify those responsible, and otherwise respond appropriately.

Wisconsin Cyber Disruption Response Strategy (2015) (Not Publicly Available)

Wisconsin Cyber Incident Annex (2015)
Established: Created as an annex to the emergency response plan.

Purpose*:* The cyber disruption response strategy establishes a standardized, flexible and scalable foundation for state agency preparation for, and response to, a threat or attack involving state networks, local government networks, and networks involved in supporting critical infrastructure.

Definition of Cyber Incident: An occurrence related to computers, servers, controls, electronic files, email systems, software, networks, or the internet requiring a response to protect life, property, the environment or the economy.

Lead Agency and Responsibilities: The Wisconsin Emergency Management (WEM) leads a unified response based on NIMS/ICS.

Incident Response Protocol: Wisconsin's incident response contains activities on mitigation, protection, and response.

Incident Response Protocol:

- *Mitigation and Protection activities:* WEM conducts public information campaigns on cyber-safety; performs employee training on IT policies; performs ongoing network and internet monitoring; and conducts intelligence gathering and analysis; and
- *Incident Response activities:* Contingent upon the cyber threat activates either a Minimal, Moderate, or Full Response. The response protocol for each level includes using "Wisconsin E-SPONDER," a secure online emergency management situational awareness tool that helps develop a common operating picture of a cyber threat/attack and documents and shares incident related information.