NASCIO
Representing Chief Information Officers of the States

CYBER DISRUPTION RESPONSE PLANNING GUIDE

NASCIO makes no endorsement, express or implied, of any products, services, or websites contained herein, nor is NASCIO responsible for the content or activities of any linked websites. Any questions should be directed to the administrators of the specific sites to which this publication provides links. All critical information should be independently verified.

This project was supported by Grant No. 2010-DJ-BX-K046 awarded by the Bureau of Justice Assistance. The Bureau of Justice of Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view of opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice.

CYBER DISRUPTION RESPONSE PLANNING GUIDE

NASCIO
Representing Chief Information Officers of the States

April 2016

State governments are at risk! Cybersecurity protection, response, resiliency and recovery dominate the agendas of chief information officers, both in the public and private sector. No organization is immune from the impacts of a cybersecurity event. From the state government information technology leaders' perspective, cybersecurity has been on the annual State CIO Top Ten priorities published by NASCIO since the inception of the list in 2006. Since that first Top Ten List was published, the frequency, magnitude and sophistication of cyber attacks has continued to increase at an accelerated pace. Possibly beyond what anyone could have imagined even ten years ago. Cybersecurity events now have the potential to significantly disrupt the business of government.

The media reports major cyber events every day. For state governments and other public sector organizations, the risk is real. The impact is expanding in terms of reach; number of citizens affected; value of intellectual capital and national secrets stolen; and business impact on industry, banking, retail and healthcare. 2014 was labeled by some as the year "everything doubled" in terms of cyber attacks, cyber crime, and cyber spending.

State government must now view cyber attacks that are more than cyber incidents and must prepare for events with significant consequences beyond the loss of data. These can be termed cyber disruptions, disasters or even catastrophes. This guide is both a practical implementation document and a call to action for states to develop state cyber disruption response plans that include: a governance structure that clearly designates who is in charge in a given event or phase of an event; development of a risk profile for state assets; collaboration among the various agencies that have cyber responsibility; and a communication plan to ensure the right people have the right information as early as possible so they can respond effectively. Integration with existing plans and protocols must be considered. Most importantly, what is clearly needed is collaboration and integration among the state CIO organization, law enforcement, homeland security, emergency management, the National Guard and the state fusion center.

The key message is that a cyber disruption response strategy and operations need to be addressed now – in advance of a cyber event that would be of such a magnitude that it could be categorized as a cyber disruption.

States need a way forward that enables state government to develop, mature, and continually test the necessary capabilities that in the best circumstances will eliminate or

limit cyber events and the effects from such events. The key word is resiliency. Vital systems and services must be built to survive a crisis. States must also continue to develop, mature and test capabilities for dealing with the aftermath of such events.

With support from the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, NASCIO has teamed with its state members, its corporate members and its allied state government associations to begin the development of a dynamic, real-time library of resources for states to use and to contribute to. This resource will build over time touching such topics as advanced cyber analytics, asset management, disaster recovery, coordination and integration with emergency management.

The following guide is a version 1.0 document that will be reviewed and updated as needed. It is a first edition dealing with cyber disruption, but is also one resource in a long line of reports that NASCIO has published on cybersecurity.

Please use this guide and contribute to the ongoing enhancement, maturity and completeness of NASCIO's library of resources dealing with cybersecurity and cyber disruption response planning. Contributors will be helping their states, their citizens, and themselves.

We thank you for your commitment and contribution.

Darryl Ackley
President
NASCIO
Chief Information Officer
State of New Mexico

Doug Robinson
Executive Director
NASCIO

Stu Davis
Immediate Past President
NASCIO
Chief Information Officer
State of Ohio

Eric Sweden
Project Director, Cyber Disruption Response Guide
Program Director, Enterprise Architecture & Governance
NASCIO

TABLE OF CONTENTS

SECTION 01

CYBER DISRUPTION PLANNING GUIDE

Key Question:

Is there appropriate support for creating, sustaining and maturing a cyber disruption response plan?

Executive Summary

The purpose of the guide is to encourage states to develop their own cyber disruption response plans. It provides guidance on what a cyber disruption is and how states should proceed in developing capabilities to plan for, prevent, mitigate and respond to such events. It makes several very strong points:

- State governments and the critical infrastructure within the state are at risk from a cybersecurity attack that could disrupt the normal operations of government and impact citizens.
- Cyber disruption response planning is essential. It is one of those aspects of government that fit in the category, "ignore at your own peril."
- Those working in this area must understand and appreciate the ultimate effects of a cyber disruption are felt by individuals, families and communities whose lives are changed. Returning to normalcy may never happen, or it may happen after much time and effort. Thus, preparing for such events must be a priority for state government, leaders and critical stakeholders.
- Governance must be in place to start and guide the process of developing capabilities related to cyber disruption response.
- Just like planning for a natural disaster, coordination and integration among state government agencies and officials is essential.
- Risk management, communications and training are high priorities for cyber disruption response planning.
- There exists either formally or informally a portfolio of threats. Those threats will move up or down the scale of threat levels throughout their lifecycle. It is conceivable that emergency management and cyber security functions are tracking and mapping the same event. Orchestration of efforts between various state government functions is essential to effective response. To support this concept this guidance document is supplemented with a cross functional process description which is a separate section of this publication.

With the realistic impacts of an event as portrayed in the guide's opening scenario, state governments must already know the potential impacts and its planned response. A clear distinction is made between cyber disruptions and cyber incidents. Cyber incidents are more numerous and routine in nature. Cyber disruptions are major events potentially involving critical infrastructure. Most important is the scope of the effects that result from a cyber disruption.

Recommendation:

Identify all partners from across government, industry and non-profits to build a network of stakeholders related to cyber disruption planning.

The guide ends with a set of recommendations for state government and an appendix with additional references. Accompanying this guidance document are the following:

- State government checklist for planning and evaluating a cyber disruption response plan
- A proforma cross-functional process description that presents how various state agencies and organizations would coordinate efforts at various threat levels.

This guidance document is a first version and will be enhanced over time with input from various state government agencies, non-profits, corporate partners and the federal government. It is anticipated that cyber disruptions will only become more sophisticated, comprehensive and devastating. State governments must put in place the necessary capabilities for prevention, mitigation, response and recovery. Those capabilities must be put in place now and continually mature going into the future.

Today's Leadership Challenge: Building State Resiliency Through Cyber Disruption, Disaster and Catastrophe Planning

You wake up in the middle of the night. There is no heat. You flip the light switch. There's no electricity. You are cold! So is the rest of your family. Your three year old is snuggling up to you and complaining, "I'm cold!" You go the kitchen to get a glass of water – there is steady low stream for a little while, then it stops!

You open your mobile device to see what news you can find – and there is no connection! Now you're worried. You're thinking, "What happened?"

Sound far fetched? Not at all. This could be the circumstance faced by many Americans on any given day now or in the future. In fact, this could also be the circumstance faced by state and local governments. This is not a scenario caused by a major storm. What could actually cause such a loss of electrical power, loss of water supply, and loss of telecommunications is a deliberate multi-faceted, well-orchestrated cyber attack. It could affect a town, a county, a state, a region or the entire country. This type of event has the potential to severely impact the economic security of our government institutions and the welfare of citizens. How can we predict, prevent, mitigate, respond and recover from cyber disruptions, disasters or catastrophes? Are states prepared?

Key Question:

What messaging is required to gain the necessary support for creating, sustaining and maturing a cyber disruption response plan?

This concern is what prompted NASCIO and the US Department of Justice (DOJ), Bureau of Justice Assistance (BJA) to explore and discuss how to shore up state capabilities in cyber disruption response planning. Those early discussions encompass a realization that the game has changed. We are no longer concerned only about cyber incidents. We are now very concerned about cyber disruptions that can cause or contribute to significant, wide-spread events that have effects on state government infrastructure, agencies, operations and eventually citizens, and that can scale from disruptions, to disasters, to catastrophes.

The effects on institutions and citizens will vary depending on their specific circumstances. The loss of critical infrastructure would be debilitating to state agencies, especially law enforcement, emergency management and first responders. The loss of electrical power for three days may be an inconvenience for a healthy 18 year old who is unable to watch and listen to their favorite music video. It would certainly be inconvenient to citizens if they could not conduct routine transactions with the government. It may be a more important disruption to a college student taking an online class. It can hamper a team of professionals from conducting a virtual meeting, but for a 75 year old woman who is on oxygen, it could be life-threatening.

The NASCIO Cyber Disruption Response, Planning and Implementation Guide is based on the premise that there are available an array of strategies, best practices, technologies and organizational models that draw from leading edge organizations from any and all sectors. The guide is intended to urge states to begin developing their own state specific cyber disruption response plans and to provide guidance on how to begin that effort.

This guide is a living document that will be continually maintained and modified over time. Even as the capabilities of cyber attacks continually increase in sophistication, state government and its partners must also continually work to increase its ability to anticipate, prevent, mitigate, recover and prosecute. Further, state government must be on a continual curve of learning, transforming, and purposefully developing its capabilities.

The Environmental Context - *Change Factors that Influence State Cyber Disruption Plan Development*

With the existing and growing dependence on information technology, state governments must continue to change how services are delivered to its constituents. This change mandates an ever increasing need for

Recommendation:

Establish positive collaboration among various stakeholders now – well in advance of a cyber disruption. There should be frequent non-crisis interaction in order to develop the necessary trust relationships that will be fully exercised during the stress of a real crisis.

more effective capabilities in cybersecurity. Current circumstances can be further characterized as follows.

- Δ Nominal fiscal recovery and nearly flat IT budgets
- Δ Need for continuity of government services during disasters
- Δ Game changing cybersecurity threats: new risks; emerging new threat targets – e.g., financial, health
- Δ New motivations for doing harm: ideologically motivated cyber threats; profit motivated cyber attacks
- Δ Maturing cybersecurity governance
- Δ Expanding funding for cybersecurity
- Δ Proactive focus on social media, mobility, analytics and cloud
- Δ New technologies such as unmanned aerial systems and the accompanying data generation from these devices
- Δ Exponential growth of data
- Δ The anticipated benefits and risks associated with the Internet of Things (IoE)
- Δ IT workforce: retirements, skills gap, recruiting challenges
- Δ Market forces of change and future role of the state CIO, CISO, CDO
- Δ Legacy modernization
- Δ Accelerated federal and state government activism, legislation, orders and directives, frameworks

Cyber disruption planning must include within its context awareness of these and other market forces, changes in citizen needs and expectations, and the leveraging of evolving technology advancements in order to plan and implement cybersecurity strategies that are up to date and relevant. Given that state government is in a period of transition between on premise and off-premise services, cyber disruption response planning must address cloud services and cross-jurisdictional partnerships that involve shared services.

Purpose of this Guide

The ultimate outcome sought through NASCIO's Cyber Disruption Response Planning initiative is the eventual development of state government *resiliency*. State government information technology is the foundation for virtually any service, any process, and capability necessary to respond to an emergency. Therefore, IT infrastructure must have such a high level of reliability and resiliency under virtually any circumstance. This includes both on-premise and off-premise technologies and services. Cloud services must be included in the purview of state cyber disruption response plans.

Key Question:

Who are key executive sponsors critical to the success of a cyber disruption response plan?

States must establish, maintain, and grow their capabilities in resiliency. Resiliency must be baked into state government enterprise architecture, all projects and all services. It must be a consideration in any purchase of technology or cloud service.

This guide presents some early targets to address in a call to action to develop state government cyber disruption response plans. Accompanying this publication is a checklist of considerations. Both documents should be considered early versions that need to be maintained and updated over time.

Resiliency: The *capacity* to *ensure* that all *vital* public services *survive* in a crisis

This report is being published in direct response to the nature of new game-changing cyber threats. Here are a few examples that demonstrate the current threat landscape:

- In 2015, one state reports 2.8 million connections blocked per day. Another state recently reported over 100 million cyber attacks per day.
- In fiscal year 2014, the Office of Cybersecurity and Communications identified 297 cyber attacks on Federal Government networks. This includes cyber attacks such as Heartbleed that targeted the White House, the U.S. Department of State, the U.S. Postal Service and the National Oceanic and Atmospheric Agency.
- Systems at Sony Pictures were hacked resulting is the capture of personal information of approximately 4,000 past and present employees.[2] The attackers took terabytes of private data, deleted the original copies from Sony computers, and left messages threatening to release the information if Sony didn't comply with the attackers' demands.[3]
- In 2014, 56 million credit cards may have been compromised in a five-month attack on Home Depot's payment terminals, making the breach much bigger than the holiday attack at Target Corporation

FEMA National Planning Mission Areas and Frameworks

Recommendation:

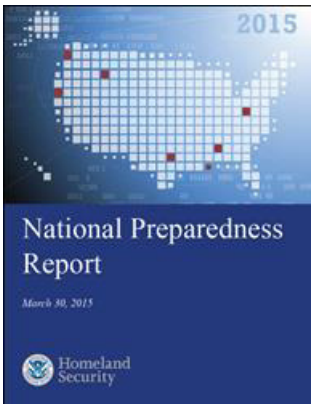
Integrate cyber disruption planning with emergency management operations.

- Chinese hackers are suspected of carrying out a "massive breach" of the personal data of nearly four million US government workers.[5]

- The most outstanding circumstance is that so many things related to cyber security doubled in 2014, that it is referred to as "the year cyber danger doubled."[6]
    - Number of public and private sector cyberattacks
    - Spending on cyberdefense
    - Cost of data breaches

2014 was "the year of cyber events," or the year "everything doubled;" 2016 may prove even worse. Cyber threats and actual attacks are continually on the rise in both number of events and the level of sophistication. Cybersecurity has maintained a position on the state CIO Top Ten Priority Strategies, Management Processes and Solutions since the inception of the Top Ten in 2006. However, no one could have dreamed possible the level of proliferation in cyber crime, the network of organizations committing such crimes, the profit motives and international espionage that have occurred in recent times. In addition, nation state attacks are now more common as attempts to compromise government networks, critical infrastructure and government contractors are reported on a routine basis.

The intent of this guide is to encourage states to devote resources toward cyber disruption planning, to share learnings and best practices, and to encourage the ongoing maturity of capabilities across the state government community. State governments have continued to mature their capabilities in *cyber incident response*. A game changer for states is the concept of cyber events that are *disruptive* in nature. This is a whole new magnitude of cyber event that cannot be properly addressed using the current cyber incident response plans.



This report will present the following:

- compare and contrast cyber incidents with cyber disruptions
- highlight of some of the elements from national frameworks that seem to be unique to cyber disruption response planning
- recommendations for moving forward

This guide is the first in a series of publications on cyber disruption response planning. It is not necessary to create a new framework that would supplant the existing and well adopted frameworks developed

Key Question:

Who are key stakeholders and partners that should be included in a cyber security response plan network?

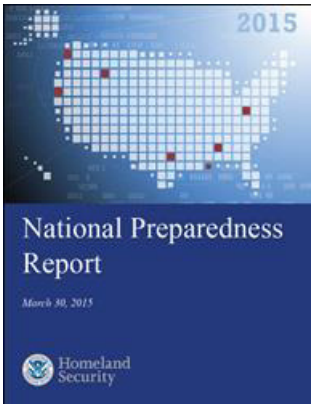
What critical infrastructure providers should be included?

What manufacturers and distributors should be included?

by NIST and FEMA. This guide will not supplant existing operating disciplines for cyber incident response planning or emergency response planning. Rather, the intent is to highlight those aspects of emergency response planning which are believed to be unique to an elevated cyber event and leverage the work from across the states as states continue to mature their capabilities in alignment with the NIST Cybersecurity Framework Functions[7] and the National Planning Frameworks[8].

Throughout this guide various *checklist elements* such as content, actions, purposes, policies, best practices and recommendations will be presented. These will constitute recommended content for a state specific cyber disruption response plan. These will be presented with a check box [☐] to indicate a cyber disruption plan element states are encouraged to consider in developing their state-specific cyber disruption plans.

What is a Cyber Disruption?
What is a Cyber Disruption Response Plan?



Before we go much further, we need to be clear regarding cyber disruptions and cyber disruption response planning. There has been a significant amount of effort devoted by the federal government and the states in dealing with this new age of national threats both man-made and natural disasters. In light of significant natural disasters such as Hurricane Katrina, Hurricane Sandy, wild land fires, record level tornadoes and flooding, the Federal Emergency Management Agency (FEMA) has created a reference library of frameworks and materials that are a primary reference for scaled disruption and disaster response planning. The frameworks were released between 2011 and 2014 in support of the National Preparedness Goal.

The National Preparedness Goal, released in September 2011, refers to the concept of *whole community* working together to be prepared for all types of disasters and emergencies.

"A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."

Recommendation:

Establish the necessary governance for a regional cyber disruption plan. Governance will clearly define lines of responsibility for advisory and decision making roles based on effects and types of cyber disruption events.

These risks include events such as natural disasters, disease pandemics, chemical spills and other manmade hazards, terrorist attacks and cyber attacks.[9]

The principles and discipline provided by these frameworks is foundational to cyber disruption planning.[10] The FEMA National Planning Frameworks are part of the National Preparedness System. There is one Framework for each of the five preparedness mission areas:

- National Prevention Framework
- National Protection Framework
- National Mitigation Framework
- National Response Framework (second edition)
- National Disaster Recovery Framework

These frameworks become relevant to cyber disruption planning because of the nature of cyber disruptions. Cyber disruptions are essentially an intersection of cyber events and a disaster and an intersection between cyber incident response and emergency management response. The Secretary of Homeland Security led an interagency effort to conduct a Strategic National Risk Assessment (SNRA) in support of Presidential Policy Directive 8 (PPD-8) in order to help identify the types of incidents that pose the greatest threat to the nation's homeland security.[11] FEMA presents two types of cyber attacks in its National Threats and Hazards Table under Adversarial/Human Caused Threat/Hazard Group.[12]

Threat/Hazard Group	Threat/Hazard Type
Natural	Animal Disease Outbreak
	Earthquake
	Flood
	Human Pandemic
	Hurricane
	Space Weather
	Tsunami
	Volcanic Eruption
	Wildfire
Technological/Accidental	Biological Food Contamination
	Chemical Substance Spill or Release
	Dam Failure
	Radiological Substance Release
Adversarial/Human-Caused	Aircraft as a Weapon
	Armed Assault
	Biological Terrorism Attack (non-food)
	Chemical/Biological Food Contamination Terrorism Attack
	Chemical Terrorism Attack (non-food)
	Cyber Attack Against Data
	Cyber Attack Against Physical Infrastructure
	Explosives Terrorism Attack
	Nuclear Terrorism Attack
	Radiological Terrorism Attack

Strategic National Risk Assessment (SNRA) Identified Threats

Key Question:

What threat sharing networks currently are in place at the national, regional and local levels?

What are the predictive capabilities of these networks?

How quickly are network members informed when on member has identified a cyber threat?

A cyber disruption either causes a disaster, or is specifically launched by a perpetrator to coincide with a natural disaster. When a cyber disruption coincides with a natural disaster or is orchestrated with another man-made disaster, first responders, hospitals, industrial partners, government and other responding organizations may be greatly hampered in their ability to respond effectively or optimally.

Therefore, it is important to distinguish between a cyber incident and a cyber disruption. A cyber incident is typically fully managed within the state CISO's purview. Whereas a cyber disruption, by its very nature, requires a coordinated response from a whole host of organizations that includes emergency management, law enforcement, homeland security, National Guard, and others.

Cyber disruption response planning is now a critical activity that must be developed and continually maintained at all levels of government and the private sector. NASCIO and others have previously published on the increasing sophistication, persistence, and magnitude of cyber attacks. A cyber disruption response plan must do more than provide response to the more commonly experienced localized cyber incidents encompassed by what most states have in place as an *incident response plan*. A cyber disruption response plan needs to address events that have a wide scope and high magnitude of effects including other service areas or industries. Several states and cross-jurisdictional collaboratives made up of state and local governments have already taken first steps in developing cyber disruption centered approaches. Examples include the state of Michigan, the state of New York, and the New England Regional Catastrophic Preparedness Initiative.[13]

Recommendation:

Establish a priority for activities based on near-term, medium term and long term time lines.

Function Unique Identifer	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID/BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processess and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST Framework for Improving Critical Infrastructure Cybersecurity

It is important to realize that certain types of cyber incidents may interfere with government's ability to respond to a variety of emergency events. Certain types of cyber incidents are of such magnitude and inter-dependence with other emergency events that we can term them as a *cyber disruption*. A cyber disruption is an event that has significant or even catastrophic *effects*. A cyber disruption is not a temporary inconvenience. A cyber disruption results in the sustained impairment of a critical capability that can lead to loss of life, health or safety; disrupt local, regional or national economy; curtail basic public and private infrastructure and services; and interfere with or limit the ability of state government to respond to the disruption itself.

While cyber attacks remain the primary concern relative to cyber disruption, a cyber disruption can be a secondary effect due to a natural disaster such as a flood, hurricane, tornado, earthquake, tsunami, mud slide, or fire, when those events destroy critical infrastructure assets such as cell towers, networks, or data centers. Such a disruption

Key Question:

What backup communications capabilities are in place to maintain communication locally, regionally and nationally?

can interfere with state government emergency response that relies on network technologies for communications, coordination and orchestration of emergency medical services, fire and rescue services, and law enforcement.

In response to the rapidly changing threat landscape, the critical dependency of information technology in support of virtually all aspects of life, the economy, government, infrastructure and the ability of the nation to respond to emergencies, and in fact the national and economic security of the United States, the President issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, in February 2013. That order directed the National Institute of Science and Technology (NIST) to work with various stakeholders to develop a voluntary framework for cybersecurity that is based on existing standards, guidelines, and practices, and with the purpose of reducing cyber risks to critical infrastructure.[14]

NIST released the first version of the Framework for Improving Critical Infrastructure Cybersecurity on February 12, 2014. NIST is continuing to enhance the framework over time. This framework will be a foundational reference going forward.

A significant cyber disruption event is defined as:

> An event or effects from events that are likely to cause, or are 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 that provide direct information technology services or enabling and support capabilities for other services; and/or threaten public safety, undermine public confidence, have a negative effect on the state economy, or diminish the security posture of the state.[15]

The class of cyber incidents that fit within the term “cyber disruption” can be described through examples such as:

- a cyber attack on the power grid leading to loss of power to a significant population;
- a cyber attack on water treatment and delivery leading to a loss of water supply to a significant population;
- cyber attacks on financial management, healthcare providers, transportation systems, education;
- a cyber attack on network capabilities leading to loss of communications which then hampers, interrupts or prevents the operation of government and requires implementation of a Continuity of Operations Plan;

- a hurricane, flood, tornado, earthquake, or other natural disaster that impairs or destroys a key infrastructure asset that then precipitates the loss of connectivity over the internet or internal network;
- natural disaster that impairs or destroys a data center which then precipitates loss of connectivity or loss of data access and requires implementation of a Continuity of Operations Plan; or
- a natural disaster that is further complicated due to an ensuing cyber attack.

Similar to electrical power generation and distribution, there are cyber assets that must be included in state government critical infrastructure key resources (CIKR). And, similar to power, the importance of these assets include the network of interdependencies that exist relative to essentially every other critical infrastructure key asset, government operations, public safety, public health, and the state of regional and national economies.

So how might a cyber disruption demand a different response than a cyber incident? How does a cyber disruption compare and contrast with a cyber incident?

The following table compares and contrasts cyber incidents from cyber disruptions. However, it is also important to understand that a cyber disruption may be initially identified as either a cyber incident or an emergency. In future, there may be hybrids of incidents and disruptions. For now, this guide will simply distinguish two types of cyber events and the appropriate scope of response planning necessary to deal with them.

Scope

Cyber Incident Response Planning

Impacts:

- a specific device / system / network
- an individual or specific customer base
- loss of specific information such as personal identifiable information (PII)
- limited in time duration (minutes to days)
- an objective of containment, restoration, recovery

Target:

- a specific database, system
- a specific company
- a specific government agency / network

Root cause:

- cyber attack
- direct, first order impact on cyber capabilities

Cyber Disruption Response Planning

Impacts:

- regional, national or multi-national
- profound detrimental effect on life within a region
- impairs or destroys a critical infrastructure asset such as a data center, power generation plant, distribution of electricity, treatment and distribution of water
- cascade, domino effects of disruptions (e.g., loss of electrical distribution leads to halting of water pumps and thus the distribution of water; without water cooling units in large facilities other equipment fails)
- extended duration (days to months)

Target:

- a population
- a region
- a critical infrastructure asset
- a certain skill, knowledge, data or information asset
- an entire industry or service or service cluster
- an entire jurisdiction
- a government function
- a government official or role

Root cause:

- multi-variant cyber attack
- natural disaster
- may be a cyber attack that takes advantage of a natural disaster

Pre Event

Cyber Incident Response Planning:
The preparation stage covers essential items that needs to be done before an incident takes place.

- It involves technology issues (such as preparing response and forensics tools), learning the environment, configuring systems for optimal response and monitoring, and
- business issues such as assigning responsibility, forming a team, and establishing escalation procedures

Creation of a cyber incident response team (CIRT). The actual composition of the team is determined by each state. Examples of CIRT membership:

- office of the state chief information officer
- state agencies
- Federal Bureau of Investigation
- The Multi-State Information Sharing Analysis Center (MS-ISAC)
- local, county police department
- state police
- fusion center

Cyber Disruption Response Planning:
The preparation stage covers all elements of a cyber incident response plan, addresses interaction among elements, and escalates to emergency response planning at some point in the life of a cyber event.

Encompasses and evaluates:

- maturity and capacity assessments
- identification of critical domains and services areas
- information sharing
- cyber analytics

Creation of a cyber disruption team (CDT). The actual composition of the team is determined by each state. Examples of CDT membership:

- includes members of the CIRT
- expands to include federal, state and local emergency response teams
- expands to include industrial emergency response
- national guard / other available resources
- fusion center
- business sector partners
- industry
- service providers

Pre Event

Identification and valuation of:

- critical systems – necessary for continuity of operations
- data and information assets
- identification, validation of authority, roles and responsibilities

Identification and valuation of:

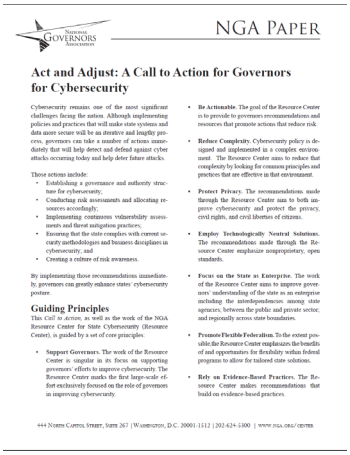
- critical infrastructure such as:
  - electrical distribution
  - water distribution
  - financial management
  - health service providers
  - communications
  - transportation
  - supply chains related to the delivery of goods and services
- interdependencies of infrastructure assets:
  - communications depends on network components such as communication lines (twisted pair, fiber, cable) or towers, and network components (switches, routers); power generation; power distribution
  - power distribution depends on power generation and communication technology
  - water treatment and distribution depend on power distribution and communications technology

Recommendation:

Identity vulnerabilities in current infrastructures including computer networks.

Overview of Recommendations – Getting Started

In concert with this report, NASCIO has created an initial checklist *Guidance for Coordinated and Integrated Cybersecurity Disruption Response Planning: Essential Elements*. This checklist was distributed for review and comment at the National Governors Association (NGA) *Summit on State Cybersecurity* held on March 30 and 31, 2015. Comments were received and the checklist was updated. The checklist is intended as a reference for states in the development of state and regional cyber disruption response plans.



NGA PAPER

Act and Adjust: A Call to Action for Governors for Cybersecurity

Cybersecurity remains one of the most significant challenges facing the nation. Although implementing policies and practices that will make state systems and data more secure will be an iterative and lengthy process, governors can take a number of actions immediately that will help detect and defend against cyber attacks occurring today and help deter future attacks.

Those actions include:

- Establishing a governance and authority structure for cybersecurity;
- Conducting risk assessments and allocating resources accordingly;
- Implementing continuous vulnerability assessments and threat mitigation practices;
- Ensuring that the state complies with current security methodologies and business disciplines in cybersecurity; and
- Creating a culture of risk awareness.

By implementing those recommendations immediately, governors can greatly enhance states' cybersecurity posture.

Guiding Principles

This *Call to Action*, as well as the work of the NGA Resource Center for State Cybersecurity (Resource Center), is guided by a set of core principles:

- **Support Governors.** The work of the Resource Center is singular in its focus on supporting governors' efforts to improve cybersecurity. The Resource Center marks the first large-scale effort exclusively focused on the role of governors in improving cybersecurity.
- **Be Actionable.** The goal of the Resource Center is to provide to governors recommendations and resources that promote actions that reduce risk.
- **Reduce Complexity.** Cybersecurity policy is designed and implemented in a complex environment. The Resource Center aims to reduce that complexity by looking for common principles and practices that are effective in that environment.
- **Protect Privacy.** The recommendations made through the Resource Center aim to both improve cybersecurity and protect the privacy, civil rights, and civil liberties of citizens.
- **Employ Technologically Neutral Solutions.** The recommendations made through the Resource Center emphasize nonproprietary, open standards.
- **Focus on the State as Enterprise.** The work of the Resource Center aims to improve governors' understanding of the state as an enterprise including the interdependencies among state agencies, between the public and private sector, and regionally across state boundaries.
- **Promote Flexible Federalism.** To the extent possible the Resource Center emphasizes the benefits of and opportunities for flexibility within federal programs to allow for tailored state solutions.
- **Rely on Evidence-Based Practices.** The Resource Center makes recommendations that build on evidence-based practices.

444 North Capitol Street, Suite 267 | Washington, D.C. 20001-1512 | 202-624-5300 | www.nga.org/center

NGA has recognized cybersecurity as a high priority and established the NGA Resource Center for State Cybersecurity in October of 2012 and in September of 2013 released *Act and Adjust: A Call to Action for Governors for Cybersecurity*. That publication emphasized three early target priorities for state cybersecurity:

- Establishing a **governance** and authority structure for cybersecurity;
- Conducting **risk assessments** and allocating resources accordingly;
- Implementing continuous vulnerability assessments and threat mitigation practices;
- Ensuring that the state complies with current **security methodologies** and business disciplines in cybersecurity; and
- Creating a culture of **risk awareness**.

In alignment with NGA, NASCIO is recommending these early targets for focusing early efforts in addressing the next magnitude cyber event – cyber disruptions.

- Governance
- Risk Assessment
- Mitigation
- Training
- Proactive Assessments
- Communication
- Response
- Recovery

The full portfolio of functions and processes for emergency management are represented in the FEMA frameworks.

Key Question:

What are key assets and roles that must be available at the various stages of a cyber disruption event?

Early Elements of Cyber Disruption Response Planning

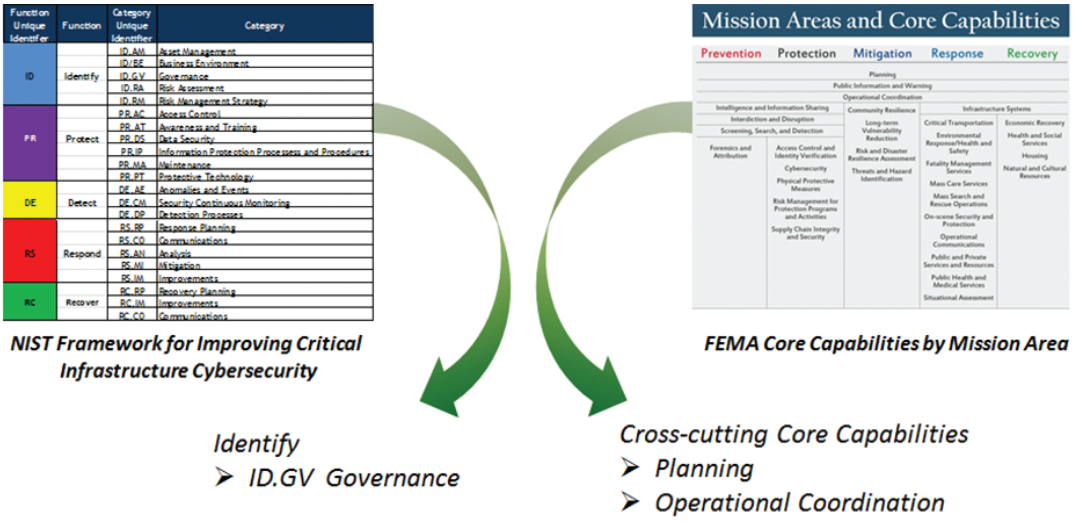
- ☐ **Organization and Governance:** determining roles and responsibilities and decision rights and rules.
- ☐ **Mitigation and Risk Assessment:** The intention is to identify what is at risk and the probability and magnitude of such risks. Mitigation strategies are designed based on identified risks. Mitigation is response focused on the thing being defended. Mitigation efforts are intended to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of the effects of cyber disruption event. Mitigation measures may be implemented prior to, during, or after an event.
- ☐ **Communication:** Communication includes internal communication for properly orchestrating resources, communicating known or anticipated threats, external communication to regional partners, and status updates to citizens and the press.
- ☐ **Response:** Formulating a specific response based on the type of disruption, its magnitude and severity in order prevent disruption if possible, to recover and restore operations.
- ☐ **Training:** Training strategy must provide the appropriate training for the various roles of the cyber disruption response team as well as every employee.

Organization and Governance - *The Cyber Disruption Team (CDT)*

As stated, organization is the starting point for developing a cyber disruption response capability. A cyber disruption team is assembled with representation from a number of organizations internal and external to state government. Once that organization is in place it will need to establish the necessary governance structure for making decisions; developing processes and operating discipline; establishing and maintaining roles and responsibilities; clearly stating who has primary responsibility at different threat levels and throughout the life of a disruption event; and the other aspects of the cyber disruption plan. The purpose of the cyber disruption team is effective execution of each step and each process in the cyber disruption response plan.

Recommendation:

Develop a strategy for continuity of communications within government and with its external partners specifically addressing the loss of telecommunications including internet and wireless networks.



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST Framework for Improving Critical Infrastructure Cybersecurity

FEMA Core Capabilities by Mission Area

Identify
- *ID.GV Governance*

Cross-cutting Core Capabilities
- *Planning*
- *Operational Coordination*

The cyber disruption response organization will have internal and external structures, roles and responsibilities. The internal dimension is the state government cyber disruption team (CDT). This team will contract and expand depending upon the effects of a cyber disruption event and the critical infrastructure key resources that have been impacted or are expected to be impacted by the event. Members and representation on the CDT will include information technology (cybersecurity, enterprise architecture, portfolio management, risk management) and executive branch agency management. Executive branch agencies will include emergency management, homeland security, and state police.

The external dimension is partnering with necessary external partners including national cyber networks, other jurisdictions relevant to mutual aid pacts, industry, universities, utilities, and non-profits. These external partners are essential to ensure well-coordinated communication, prediction, analysis, detection, response and recovery regarding cyber disruption threats and to maximize available resources including funding.

Due to the scope and potential effects of a cyber disruption, effective preparation and response must involve a collaborative effort involving the public and private sector. The state government cyber disruption plan must be planned and orchestrated by a rather comprehensive list of partners. To be successful, any collaborative initiative must have an *owner or director* that ensures participation, reports on progress, oversees the organization and operating discipline, and engages new members. It is recommended that that owner / director be the State Chief Security Officer (CISO) and that the role will include responsibility for the overall administration and maintenance of the cyber disruption

Key Question:

What are the priority assets and a backup/ recovery strategy for these assets?

Assets critical to continuity of government

Assets critical to responding to emergencies and disasters

response plan and the monitoring and reporting of progress. Any state cyber disruption response plan must be developed and maintained in collaboration and in partnership with the state emergency management, homeland security, state police, fusion center, and the National Guard. The particulars of any such organizational arrangements are state specific.

Given the scope of what we have termed a cyber disruption, strategic partnering is essential to planning and orchestrating effective preparedness, detection and response capabilities.

☐ ***Governance***

Organizational structure, roles and responsibilities must be clearly specified in the cyber disruption response plan. Integrated with that structure is the concept of governance. Governance refers to decision rights and clearly specifies who has responsibility for what decisions. In a crisis situation, it is imperative that everyone involved knows the following:

- ☐ Who is in charge of what policies, processes, people and technologies
- ☐ Who is conducting ongoing environmental scan for emerging threats
- ☐ Who is conducting ongoing network scans for potential and real attacks
- ☐ Who is responsible for data management, information sharing and cyber analytics
- ☐ Who is responsible for ongoing training of all employees and CDT staff
- ☐ Who is responsible for communication internally and externally
- ☐ Who will organize a team for a specific event
- ☐ Who is monitoring all events while looking for possible orchestration on the part of the enemy
- ☐ Who will provide expert assessments during actual events
- ☐ Who will make the decision to escalate an event from a cyber incident to a cyber disruption

Recommendation:

Develop communication and coordination procedures to ensure timely and effective response in the event of a cyber disruption.

- ☐ Who will transfer / receive responsibility when a cyber incident is elevated to a cyber disruption
- ☐ Who will provide expert recommendations
- ☐ Who will make the decision to de-escalate an event down from a cyber disruption to a lower threat level
- ☐ Who has the authority and responsibility for making decisions

Governance entails the internal organization of state government and, given the scope of a cyber disruption, must involve external partners.

☐ ***Authority for a Cyber Disruption Plan – A Shared Responsibility***

A cyber disruption plan should apply to all State agencies, boards, commissions, and departments within the state executive branch and to others as designated by the Governor or Director of the Emergency Management as well as local governments.

The primary responsibility for development, implementation and ongoing maturity of the state cyber disruption plan resides with the state chief information security officer (CISO). Due to the nature of cyber disruption events there must be a shared responsibility with the Director of the Department of Public Safety or Emergency Management for leading the cyber disruption response plan. Other organizations may be involved depending state specific legal provisions and policies.

The state emergency management function has very broad responsibility for all hazards event management including orchestrating effective response. Thus, the overall authority and responsibility over emergency events is the director of emergency management. That responsibility includes providing guidance and direction for overall emergency response and disaster recovery activities.

The ultimate authority for cyber disruption planning is the governor of the state or territory.

- ☐ Roles and responsibilities
  - ☐ See NASCIO's *Cyber Disruption Response Plan Roles and Responsibilities*
- ☐ Authority – executive orders, directives and statutes
  - ☐ citation of executive orders and directives
  - ☐ citation of statutes

Key Question:

Do we have appropriate interoperability between cyber incident response and emergency management functions? Are key roles and resources mapped to a cross functional process that clearly describes how they will interact and be deployed at various threat levels?

☐ ***Partnering – State Government Collaborative Networks***

A major emphasis in effective cyber disruption response planning is establishing the necessary partnering to ensure a well orchestrated response that taps the various expertise and capabilities of state government, service providers, industry, utilities, academia, and various centers of excellence to ensure an optimum response. Cyber disruption plans must necessarily be cross-boundary, holistic and regional. Based on how this guidance document has defined cyber disruptions it is anticipated that such events would involve effects that impact regions.

Key to strategy development are considerations for continuity of operations, continuity of government and government services, and the necessary supply chains that service operations. Further, due to the interdependencies of infrastructure cyber disruption response plans can be expected to require orchestration across multiple infrastructures including electrical power generation and distribution, natural gas distribution, fuels distribution, water treatment and distribution, telecommunications, public health, hospitals, agriculture and food distribution, transportation, banking and finance, government services, manufacturing, materials and waste, dams and levees, chemical facilities, postal and shipping, and commercial business.

This network of partners should be brought together now. Initial conversations will be focused on awareness, current vulnerabilities, potential scenarios and the effects from the scenarios. As with most things, communicating and collaborating is the necessary first step. Going forward the recommendations from this report and those referenced in the appendices can be used to develop tactical and strategic cyber disruption response plans. Then such plans must be exercised to test them. Learnings from such exercise must then be used to continually make improvements.

Of great concern are the interdependencies, supply chains, and potential domino effects that can occur with the initial disruption of one infrastructure base leading to secondary and tertiary effects in other infrastructures.

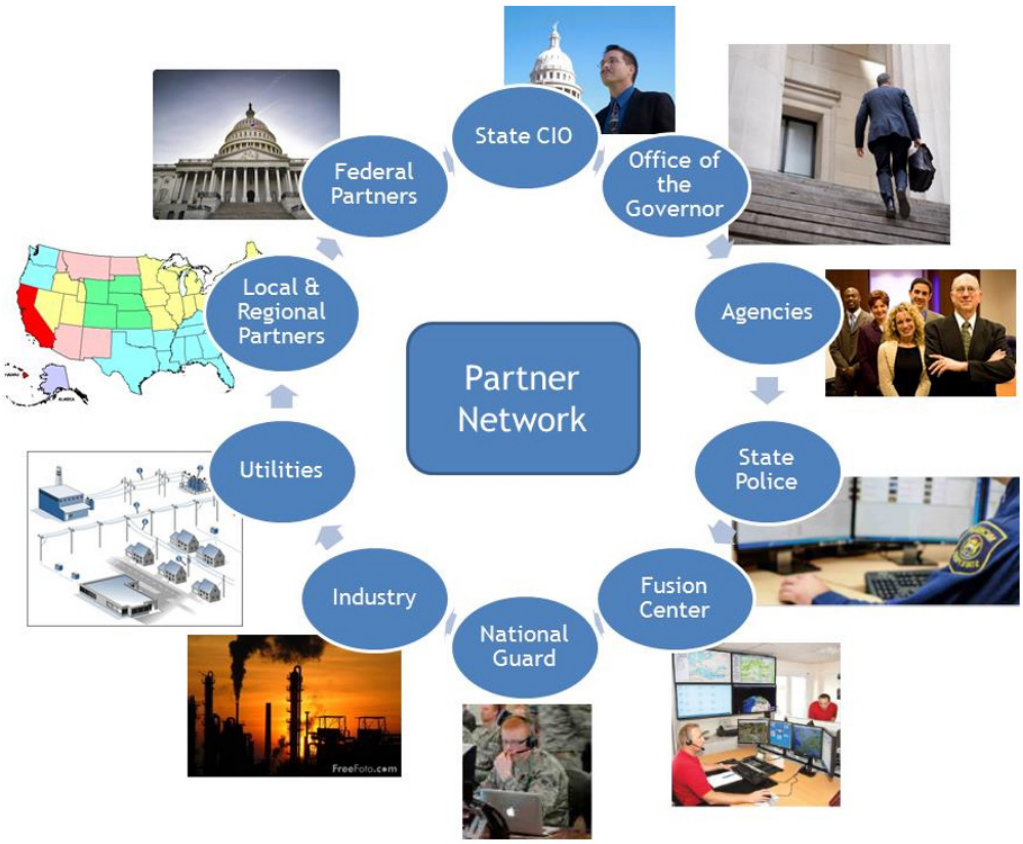
Depending on the effects that result from a cyber disruption, the cyber disruption response team will require representation from a wide array of partners in understanding scope and impact as well as formulated proper mitigation and recovery plans. It is imperative that state government engage this list of partners now to begin formulating cross-functional operating discipline for informing all partners of any emerging or actual threats; mitigation and response scenarios; and sequestering the necessary resources that will provide the means for communication

Recommendation:

Develop contingency plans, alternative action plans considering secondary effects of regional emergencies and secondary effects of cyber disruptions.

and coordination in the event of a cyber disruption. There should also be a review of relevant statutes and regulations unique to the state that may have implications for partnering.

Necessary members for any given event will depend on the effects either anticipated or actually experienced. Considering potential escalating domino effects, membership should be more inclusive. Cyber disruptions can in fact impact any number of critical infrastructure key assets in a state, key public and private sector services, as well as challenge the ability of government to maintain government operations.



Cyber Disruption Partners

In advance of any event, a collaborative network must be built that clearly delineates the roles of each partner. Important members of any state cyber disruption communications network include regional and national organizations that are already in place to facilitate situational awareness and information exchange with respect to cyber issues.

Key Question:

When was the cyber incident and cyber disruption response plan last tested through a tabletop exercise?

These include:

- The National Cybersecurity and Communications Integration Center (NCCIC),
- The Multi-State Information Sharing Analysis Center (MS-ISAC)
- State specific Information Sharing Analysis Center ([state] – ISAC)
- The United States Computer Emergency Readiness Team (US-CERT)
- The National Fusion Center Association Cyber Threat Intelligence Subcommittee (NFCA-CTI)
- The Information Sharing and Analysis Organization (ISAO)

☐ ***Regional Collaboratives***

A state may be a member of a regional or peer network of like jurisdictions that share information with a closer cohort of communication partners. Such communities of interest (COI) are typically put in place to receive and communicate cyber-related information, and coordinate emergency response activities among regional catastrophic planning area (RCPA) jurisdictions during catastrophic incidents.

> *NASCIO has published a series of guidance documents specific to forming cross-jurisdictional collaboratives including governance, funding and other best practices that make such arrangements successful. See www.nascio.org/advocacy/collaboration to access this library of references.*

In the event of a cyber disruption, each partner knows exactly what to do. An important discipline for partnering is sometimes referred to as a Concept of Coordination which clearly articulates roles, responsibilities and orchestration of roles and partner organizations in preparing for mitigation, response and recovery. Activities within such a partner network may include:

☐ Alternative modes of communication

☐ Sharing of resources

- ☐ cross-agency and cross-jurisdictional mutual aid pacts
- ☐ formal service agreements

☐ Establishing cold, warm, or hot backup sites

☐ Coordinating information sharing for the purpose of:

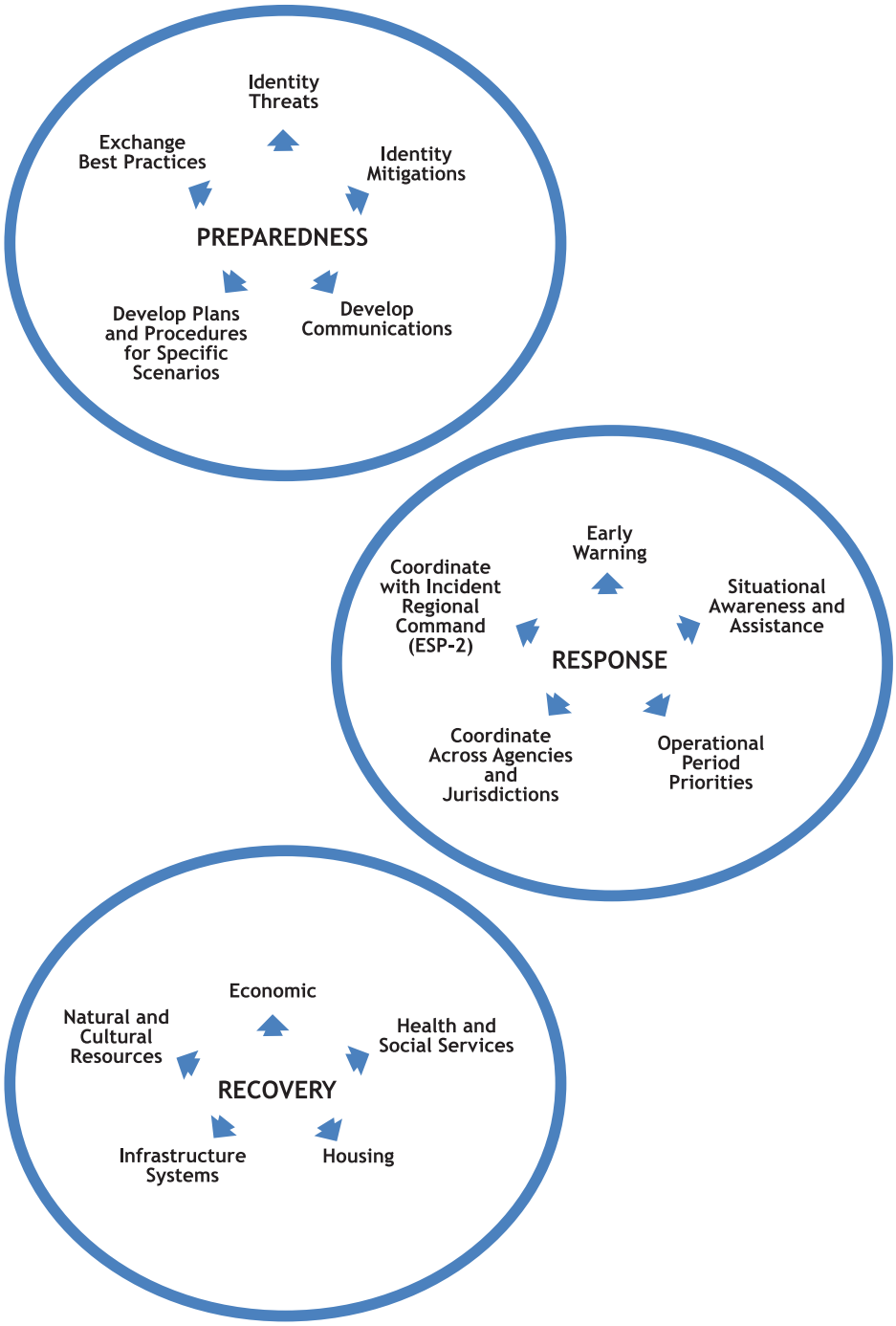
- ☐ preventing and protecting state critical infrastructure key assets including cyber assets
- ☐ detecting cyber threat and actual attacks

Recommendation:

Identify what resources can be brought to bear from across the cohort of partners based on scenarios and effects.

- ☐ analyzing cyber threat potential and threats
- ☐ responding to cyber disruptions
- ☐ resolving and recovering from actual cyber disruptions

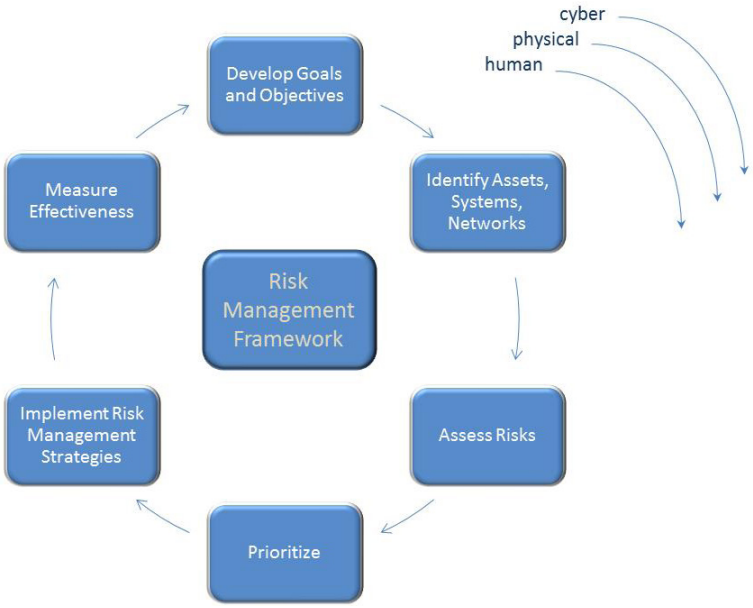
Coordinated Activities Across a Regional Cyber Disruption Initiative



Key Question:

How long will it take for our jurisdiction to restore the delivery of power, water, natural gas, internet, sewage treatment, transportation?

Mitigation - Risk Management

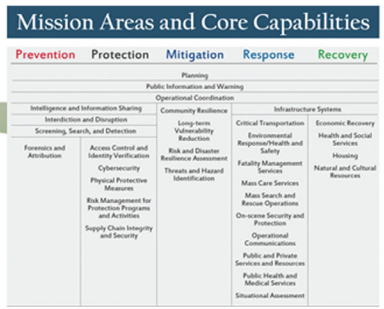


Risk Management Framework[16]

The risk management framework provides a graphical representation of the steps for inventorying, assessing and protecting cyber assets, physical assets and personnel.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processess and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST Framework for Improving Critical Infrastructure Cybersecurity



FEMA Core Capabilities by Mission Area

Identify

- *ID.RA Risk Assessment*
- *ID.RM Risk Management*

Protection; Mitigation

- *Risk Management for Protection Programs and Activities*
- *Risk and Disaster Resilience Assessment*

Recommendation:

Carefully examine supply chains, particularly those that are relied upon by all partners. If the supply chain is broken for one partner, that is most likely the circumstance for other partners.

State government's critical infrastructure systems are vast, interconnected, interdependent networks. No single enterprise, public or private, can afford the necessary resources to eliminate all risks to the continuity of public and private sector services and government. Some states have created cross-jurisdictional collaboratives that can leverage the resources of multiple stakeholders to gain some advantage. An example of this is the Michigan Cyber Disruption Response Strategy. However, even these collaboratives are not able to remove all risk. Therefore, each organization must individually employ a methodology for inventorying, assessing and protecting cyber assets, physical assets and personnel. Part of this exercise is to identify the criticality and priority of roles, systems, processes and assets. This includes the vulnerabilities, potential for attack, and strategies for managing the respective risk profile.

☐ **Risk Assessment**

Risk assessments will be the first step to identify critical assets, the potential risks and the level of risk. Risk assessment involves the development of a measure of risk based on the evaluation of the threat, vulnerability and consequences associated with an attack on a target, such as critical infrastructure. Risk assessment is necessary for risk management and typically involves the following steps.

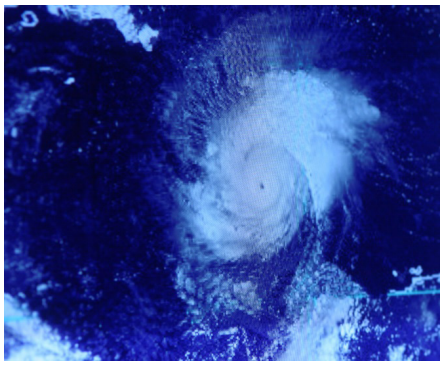
- ☐ Identify critical infrastructure and key resources
- ☐ Identify and assess threats to the subject infrastructure
- ☐ Identify the vulnerabilities of the target infrastructure associated with the identified threats
- ☐ Evaluate the consequences of a successful attack on the subject infrastructure
- ☐ Determine the risk to the subject infrastructure based on the aforementioned factors
- ☐ Identify means of reducing risk to subject infrastructure
- ☐ Evaluate the resources available to mitigate risk
- ☐ Develop a risk management strategy taking into account the risk priorities and resources available.

Common methods for risk assessment include the use of subject matter experts and the scoring of risk characteristics based on relativistic scales. Additionally, penetration testing or "red team" techniques may be used

Key Question:

What training is currently in place for existing cyber security staff? What new training should be added to shore up capabilities to support a cyber disruption response plan?

to uncover vulnerabilities and test security of potential targets, yielding data that may be used to develop risk assessments and mitigation priorities.



A common method of risk evaluation is the use of relativistic methodologies. In this approach, various scales are used commonly across all evaluated targets and targets are given a score based on the assessor's determination. Often, these risk assessments are conducted by individuals with expertise in the given sector in order to support the evaluation's integrity. These scales are typically represented in one of two ways, either by a scoring scale which applies points to different vulnerabilities which are later totaled, or by percentage. In the case of percentage the decision factor is often represented as (0,1), meaning the factor should be rated as 0% probable (0) to 100% probable (1).

For example, the threat of a vehicle borne improvised explosive device at a particular target site may be assessed by an expert to be 85% likely (.85). The factor can then be applied in a formula upon which the method is based.

$$R = T \times V \times C$$

Where:

- R= Risk (Expected Loss)
- T = Threat
  - (0,1)
  - Likelihood of a potential type of attack Intent and capability of the adversary
- V = Vulnerability
  - (0,1)
  - Likelihood or probability of successful attack
- C = Consequence

A risk assessment will identify all Critical Infrastructure and Key Resources and the primary and secondary effects of the loss or impairment of those assets. Risk assessments will look at the secondary and tertiary effects when key resources are lost or impaired. These resources include key personnel. This will include public health, public safety, economics, and the continuity of government operations. For example, if internet connectivity is lost, there will need to be secondary and tertiary operating discipline for maintaining communications across necessary government operations using alternative means.

Recommendation:

Insure backup communications networks are ready to launch and that such networks can sustain for some period of time. Over time that sustainability should be continually improved.

Risk Assessment Table				
Asset or Process	*Threat X*	*Vulnerability X*	*Consequence =*	*Risk*

☐ **Proactive Assessment**

Proactive Assessment is an ongoing surveillance of the current threat landscape that includes a predictive component to anticipate what threats are emerging. The best scenario is where a cyber attack is anticipated and prevented. This element entails ongoing real-time / near real-time assessment of the threat landscape, looking for patterns related to external probing of networks, ongoing intelligence gathering from across the partners, and updates on current threats encountered by other organizations. Additionally, this element will mature to include predictive analytics moving as forward into the future as is technically and economically feasible. Thus, moving the "response" to the forward side of the curve emphasizing less reactive and a more proactive stance. This is essentially the "Star Wars" capability in cyber defense. Coordination occurs along the entire operational process. Different partners will assume more emphasis as appropriate for each process step.

Another necessary aspect of proactive assessment is an environmental scan of the ideologies and cyber-crime incentives and opportunities that exist with a clear understanding of the agendas for these ideologies. There are ideologies that have very clear agendas for bringing down the United States through various means. A proper defense and offense can not be formulated without understanding the enemy. This was a very necessary ingredient in the United States defense strategy during the cold war. Today there are many more nation states and non-nation state networks of terrorists that are aggressively targeting the United States, its interests, its economy, and its citizens. The proactive assessment must include an ongoing vigilance of these threats and their underlying ideologies. A necessary part of an effective defense will be to focus on those underlying ideologies, challenge them, and present compelling debate that will promote freedom and liberty. Without addressing the underlying beliefs and perceptions that drive terrorism, economic

Key Question:

What modifications should be made to the NASCIO cyber disruption checklist and the NASCIO cross functional process to adapt those resources to our circumstances?

exploitation and cyber attacks, cyber disruption plans will remain tactical, reactive and only partially successful.

Situational awareness is tightly coupled with communication. Current and emerging threats will be identified and assessed from any number of partners that maintain a capability for identification and analysis. Some partners will have sophisticated predictive cyber analytics for surfacing and analyzing patterns. It is important to maintain appropriate interaction among partners based on the analysis of threats. With many eyes on a circumstance, some will see patterns previously missed by others. Organizations should identify others that may have the same types of systems (e.g. water systems, electric utilities, health care, etc.) that would benefit from sharing security controls and strategies.

☐ ***Proactive Assessment Activities:***

- ☐ Identify vulnerabilities and the attractiveness of potential targets

- ☐ Identify threats and vulnerabilities to IT networks with respect to emergency management objectives and priorities
- ☐ Monitor all cyber incidents for possible escalation to cyber disruption status
- ☐ Identify mitigations (e.g. plans, procedures, hardening measures, etc.) for threats and vulnerabilities
- ☐ Employ predictive analytics to anticipate emerging threats including the magnitude and probability
- ☐ Develop plans and procedures to address specific disruptions. Employ related emergency support functions, agencies and other jurisdictions as indicated by the type of threat
- ☐ Build and continue to update a scenario portfolio
- ☐ Build and continue to maintain a portfolio of best practices and lessons learned
- ☐ Address potential cyber disruption events in the risk assessment and risk management for any new project, program or management initiative

Recommendation:

Develop test plans for coordinating response across several or more infrastructures.

- ☐ Integrate cyber disruption risk assessment and risk management with the enterprise portfolio including systems and information assets
- ☐ Classify systems, information assets and roles according to importance in protecting and restoring, as well as the sequence of restoring in the event ofa cyber disruption
- ☐ Working with federal agencies maintain an environmental threat landscape of current and emerging threats

Communication

Communication is possibly the most critical element of a cyber disruption response plan. This element is critical to initial notifications, assessment and ongoing monitoring of the magnitude and reach of a cyber attack, operational coordination to deal with primary and secondary effects, and cross-jurisdictional partnering. Communication is the first action step toward the sequence of coordinating the various stakeholders' operating disciplines related to situational awareness, containment of a threat, mitigation, emergency response, continuity of government, recovery, and strengthening.

Two dimensions of communications are the *organization and coordination* dimension, and the *technical* dimension. Organization and operational coordination for any emergency rely upon the Web-based Emergency Operations Center. However, if the targets of a cyber attack are the national, regional or local network, communications will rely upon alternative means for communications such as state and local radio communications systems. One question that arises is the reliability of such systems.

- ☐ Are the batteries properly maintained for backup radios?
- ☐ Has the state radio communications system been tested?
- ☐ How long will such a system actually work if power distribution has been shut down by a cyber disruption?

Key Question:

Is your state currently using national frameworks for planning, implementing and testing capabilities for cyber disruption response planning?

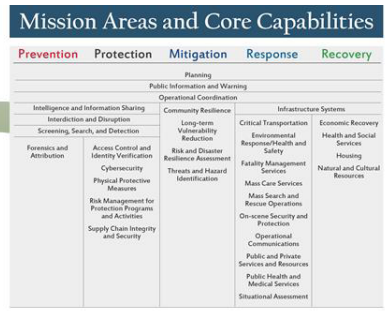
NIST

FEMA

Questions like this must be asked now and the necessary resilience and remediation put in place.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID/BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processess and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST Framework for Improving Critical Infrastructure Cybersecurity



FEMA Core Capabilities by Mission Area

Respond
- *RS.CO Communications*

Recover
- *RC.CO Communications*

Cross-cutting Core Capabilities
- *Public Information & Warning*

Prevention; Protection
- *Intelligence Information Sharing*

Response
- *Operational Communications*

Communications is key throughout all phases of a single cyber incident, a combination of cyber incidents and a cyber disruption. Communication is tied to governance. Governance will define decision rights of the various stakeholders for all stages in a cyber disruption response plan. At various points along the cyber disruption process different roles and different stakeholders will play a more dominant role based on the actual scenario and the actual effects. This must be clearly determined in advance of any cyber disruption event. As those roles and responsibilities change so will the responsibility for initiating communications among the stakeholders.

☐ ***Technical Communications***

The choice of technology and vehicle for communications includes the following:

☐ Telephone
☐ Cell phone
☐ e-mail
☐ Fax
☐ 800 MHz radio
☐ SATool
☐ HAN / Dialogics
☐ Dialogics (emergency notification system)

Recommendation:

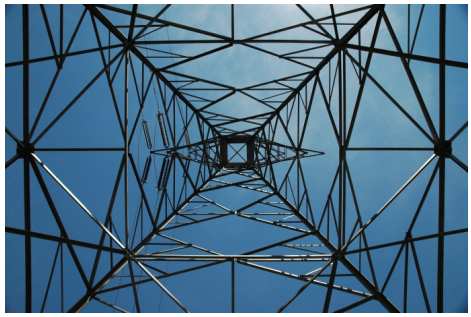
Begin to identify tactical and medium term strategies for addressing loss of power and telecommunications. Consider developing regional and local power grids that are isolated from the internet and would provide dependable power in the case of a blackout or brownout. Such a regional grid would be developed under cross-jurisdictional collaborative.

- ☐ WebEOC
- ☐ ARES
- ☐ Siren systems
- ☐ Sound trucks
- ☐ Television and radio networks
- ☐ Courier

☐ ***Organization and Coordination – The Public Information Plan***

The public information plan is essentially the strategy for communicating with citizens and the press in order to provide the appropriate messaging regarding emerging threats, initial alerts, ongoing updates and closure of events. It must be remembered that any such messaging is public and as such is harvested by the perpetrators of a cyber disruption in the case of cyber disruptions caused by cyber criminals. Cyber disruptions can also occur due to natural disasters. In the latter case, communication strategy must be coordinated with the state emergency management in order to have a coordinated and consistent message. That said, cyber disruptions due to cyber criminals can be anticipated to create a domino effect that precipitates other types of emergencies such as loss of electrical power, water, telecommunications and other infrastructures and supply chains.

A messaging strategy should be established in advance of any real emergency. Protocols and even the wording of messaging must be accurate and provide the necessary information so citizens know how to prepare prior to a cyber disruption and how to both gain assistance and provide assistance during an event. Coordination activities for public communications is best governed and managed through the formation of a joint information system (JIS) that acts on behalf of all stakeholders. Specific circumstances may require establishing a joint information center (JIC). The primary benefit of this concept is that incident command, the media and the public receive accurate, timely and coordinated emergency information. It is essential that the JIS concept determine communication strategies throughout the emergency and activation of the JIC, as these concepts work simultaneously.



Joint Information Center (JIC): A facility established to coordinate all incident-related public information activities. It is the central point of contact for all news media at the scene of the incident. Public information officials from all participating agencies should collocate at the JIC.

Joint Information System (JIS): Integrates incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, timely information during crisis or incident operations. The mission of the JIS is to provide a structure and system for developing and delivering coordinated interagency messages; developing, recommending, and executing public information plans and strategies on behalf of the incident commander; advising the incident commander concerning public affairs issues that could affect a response effort; and controlling rumors and inaccurate information that could undermine public confidence in the emergency response effort.

The mission of the joint information center is to:

- ☐ Provide a structure and system for developing and delivering coordinated interagency messages
- ☐ Develop, recommend, and execute public information plans and strategies on behalf of the incident commander, state CIO, state CISO, and/or state privacy officer
- ☐ Advise the incident commander concerning public affairs issues that could affect a response effort
- ☐ Control rumors and inaccurate information that could undermine public confidence in the emergency response effort
- ☐ Deliver critical messages to the public that is timely and accurate
- ☐ Create messaging that conveys confidence and avoids public panic

- ☐ ***Joint Information Center Scope:***
- ☐ Creation of joint information center (JIC) for authoring and coordinating the distribution of all communications
- ☐ Emergency public information actions before, during, and following any emergency will be determined by the characteristics of the cyber disruption event, State agencies affected, or as perceived by the public

Recommendation:

Develop, maintain and test a cross functional process flow that describes how stakeholders will interact at all threat levels. A starting point for this effort could be existing cross functional process flows for cyber incident management. Such a process could be scaled up to include all necessary players to deal with a cyber disruption.

- ☐ A significant emergency public information response will involve the many state, local, Non-Governmental Organizations (NGO), and private sector agencies that comprise the list of stakeholders. The governance structure identifies those agencies and their responsibilities

- ☐ For purposes of the state cyber disruption response plan, the public information officer (PIO) in the office of the state CIO is the named primary PIO. Other stakeholders will also have a primary PIO for communicating aspects of any emergency that are related to their agency, emergency support function, organization, company, or NGO. It is imperative that during a cyber disruption event that the PIOs from these stakeholders remain coordinated through the formation of joint information center (JIC)

- ☐ Resource requirements, including staffing, communications technology, equipment, office supplies, and office facilities required will be tailored to the type and magnitude of each specific disaster and full, or partial activation of this plan will be addressed on a case-by-case basis

- ☐ Additionally, resource requirements will shift as the incident moves through the various phases of the cyber disruption process.

- ☐ ***Rules of Conduct:***

The following are characteristics that should be maintained as standards of behavior or rules of conduct related to communications during all phases of a cyber disruption response process.

  - ☐ The public needs timely and accurate information for protection of life and property during a response to and the recovery from a disaster or emergency situation

  - ☐ To reduce inaccuracies and misinformation, the State will initiate a JIS to coordinate information with participating local, state, federal agencies and other stakeholders.

  - ☐ Based on the urgency of the situation and the need for inter-agency cooperation, agencies should attempt to coordinate emergency public information through the Governor's Office

  - ☐ Local jurisdictions will provide immediate and vital information to the public regarding response and recovery activities

- ☐ At no time will a news release from any state agency conflict with news releases from local government
- ☐ All efforts will be made to ensure, through active communication, through sharing of information, key messages and drafts to ensure consistency of messages at all levels
- ☐ Under the JIC concept, each agency representative has the commitment to share and coordinate information with all other participating agencies and stakeholders prior to its release to the media and public
- ☐ A JIC may be initiated through technological means when geographical restrictions, incident management requirements, and other limitations preclude physical attendance by public information officers/liaisons at a central location
- ☐ The Emergency Alert System (EAS) may be utilized by state and local jurisdictions to broadcast a public alert to specific jurisdictions.
- ☐ The overarching goal of a JIS is to have one message distributed by multiple sources and to drive traffic to lead agency/official sources for information to ensure consistency of messages for evolving incidents.

☐ ***Assumptions:***

- ☐ It is anticipated that a variety of federal, state and local agencies, as well as private sector and non-governmental organizations, may potentially become involved in any cyber disruption event. Each organization should use internal public information plans which should include the application of the JIC
- ☐ It is also assumed that individuals charged with PIO responsibilities may also be responsible for a variety of aspects of incident management, as determined by resources and staffing available
- ☐ The JIS and the JIC are both vehicles upon which the larger, Emergency Support Function (ESF) #15 is built and, while these mechanisms accommodate the breadth of activity under ESF #15, they do not represent the sum total of actions and area responsibilities of that function (See Appendix C for full list of ESFs)

Recommendation:

Incorporate resiliency measures into the enterprise portfolio for processes, systems, data and information assets, hardware, cloud services, shared services. Attribute the level of criticality for all IT assets.

- ☐ The JIC is a central, physical location where the informational needs and demands of the public, media and incident commanders can be supported, the overriding concept of the JIC recognizes that each individual will continue to bring expertise from their own agency, will continue to represent the needs of their own agency as assigned by that agency, while receiving the benefits derived from coordinated information.
- ☐ Under the JIS / JIC concept, each agency representative has a commitment to share and coordinate information with all other participating agencies prior to its release to incident command, the media and the public.
- ☐ At no time should any agency determine or approve information outside their purview of responsibility or assignment within JIS or JIC
- ☐ The JIC is designed only as a coordination, analysis and dissemination point; agency information must be approved within relative command structures prior to reaching the JIC

☐ ***Recommendations***

- ☐ Develop communication and education to raise awareness across state agencies and external partners regarding the current threat landscape, the interdependencies of infrastructures, the necessity of developing effective strategies for cyber disruption response plan communications.
- ☐ Develop communications strategy for internal and external lines of communications. Strategy will include the aspects of warnings and the status of real threats (emerging, actual, sunset)
- ☐ Develop communications means and methodologies to enable intra- and extra-jurisdictional transactions

Response
Detect, Analyze & Classify, Formulate Response

This aspect of the cyber disruption strategy will engage the cyber incident response strategy. The CDT is continually monitoring for significant or catastrophic events. The cyber incident response team may actually be the first team that identifies an emerging threat. This will require some method for classifying an event in terms of severity and magnitude. An event may be reclassified throughout the event lifecycle as the threat is identified, new information is gained regarding the nature of the event, measures are taken to prevent, dismantle, contain, and eliminate a threat.

By its very nature, a cyber disruption will typically be initially identified through cyber incident management. A cyber disruption is defined as having inherent scope and magnitude that require integration of cyber incident, cyber disruption response and emergency response.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID/BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processess and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST Framework for Improving Critical Infrastructure Cybersecurity

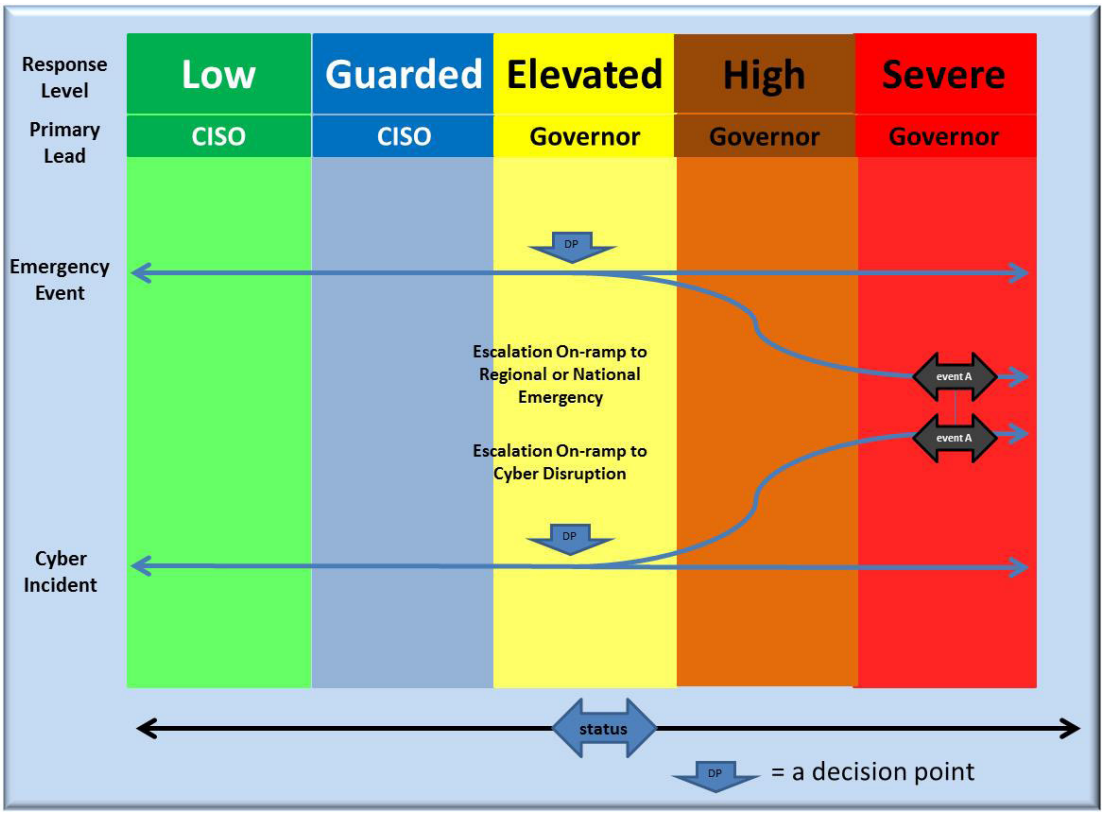
FEMA Core Capabilities by Mission Area

Response *Response*

The following graph presents a method for classifying an event and the interoperability between cyber incident, cyber disruption and emergency management. Note that an event may be moving along the emergency management and the cyber incident curves at the same time. That is, some events will have been identified by both functions. It may be initially classified differently and treated as separate events. However, through ongoing collaboration emergency management and cyber incident may judge that the two events have such characteristics to be the same event.

Recommendation:

Incorporate resiliency requirements into every project, program and management initiative.



Interoperability between emergency management, cyber incident and cyber disruption management

At some point during the lifecycle of an event, it will be decided that the event is of such a scope and magnitude that it should be classified as a cyber disruption and thus require invoking the cyber disruption response plan. Such a plan will sequester a broader portfolio of experts, agencies, cross-jurisdictional partners, industry and non-profits as presented earlier in this report in order to characterize the event and orchestrate a coordinated response. The coordinated response will execute on a pre-established concept of cooperation, be triggered by specific effects of the event, and may be elevated to a national emergency based on the process.

- ☐ Monitor events and share and collect information among internal and external partners that may indicate the development of a catastrophic cyber incident
- ☐ The event will first have to be classified as to whether it is a cyber incident which is the broader category of events, or the specialized case of a cyber disruption

- ☐ Provide situational awareness and assistance to internal and external partners during a catastrophic incident as necessary and technically feasible. There may be multiple incidents or disruptions occurring simultaneously. It may not be feasible to provide support other than communications and information sharing with external partners.

By this point in time the disruption may have reached such a level of scope and magnitude that leadership will come primarily from the emergency management team (EMT) or the office of the Governor. The example above presents the primary lead as moving to the governor at the elevated threat level. Actual determination of the lead role is state specific.

Depending on state specific emergency response plans, when an event has reached a trigger point threat level the cyber disruption response plan should include the following provisions:

- ☐ Provide situational awareness and subject-matter expertise and solutions for an Incident/Unified Commander and his/her General Staff during a response

- ☐ Assist the EMT with understanding the technical and operational issues regarding cyber-related assets and networks, critical infrastructure key assets, magnitude and scope, anticipated duration, effects on the various ESFs

- ☐ Assist the EMT with developing priorities and objectives of a long-term response to a catastrophic incident. Objectives and activities become the key elements of an action plan for a determined operational period, set out for the EMT Incident Action Plan (EIAP)

- ☐ Coordinate IT-related intra- and inter-jurisdictional response activities pursuant to a EIAP

- ☐ Coordinate with the EMT and state Emergency Support Function 2 (ESF-2) to procure critical cyber-related resources

- ☐ Engage alternative communication channels as necessary. If the disruption has taken down the internet, the web emergency operations center (WebEOC) will not be available for communication and coordination. Alternative means will need to be employed such as the statewide radio network. That means radios must be operational.

Specific cyber response procedures to limit the effect of a cyber disruption, or protect cyber assets from assault should include but not be limited to the following:

- ☐ Data Backup Action Plan
- ☐ Disaster Recovery / Business Continuity Plan
- ☐ Halt Key Processes Plan
- ☐ Equipment Shutdown Plan
- ☐ Log File Recovery Plan
- ☐ Initiate alternative power generation
- ☐ Initiate alternative cooling system
- ☐ Switch over to backup cold, warm or hot site
- ☐ Isolate vital records
- ☐ Execute mutual aid pact(s)
- ☐ Switch over to state wide radio network or short wave network for communications

During the detection and analysis of cyber incidents or disruptions, critical infrastructure owners and operators may suspect or discover criminal activity. It is essential that in the process of defending public and private networks in the state that we also root out the criminal elements that perpetrate such crimes.

- ☐ State Police may have established a state Cyber Command Center.

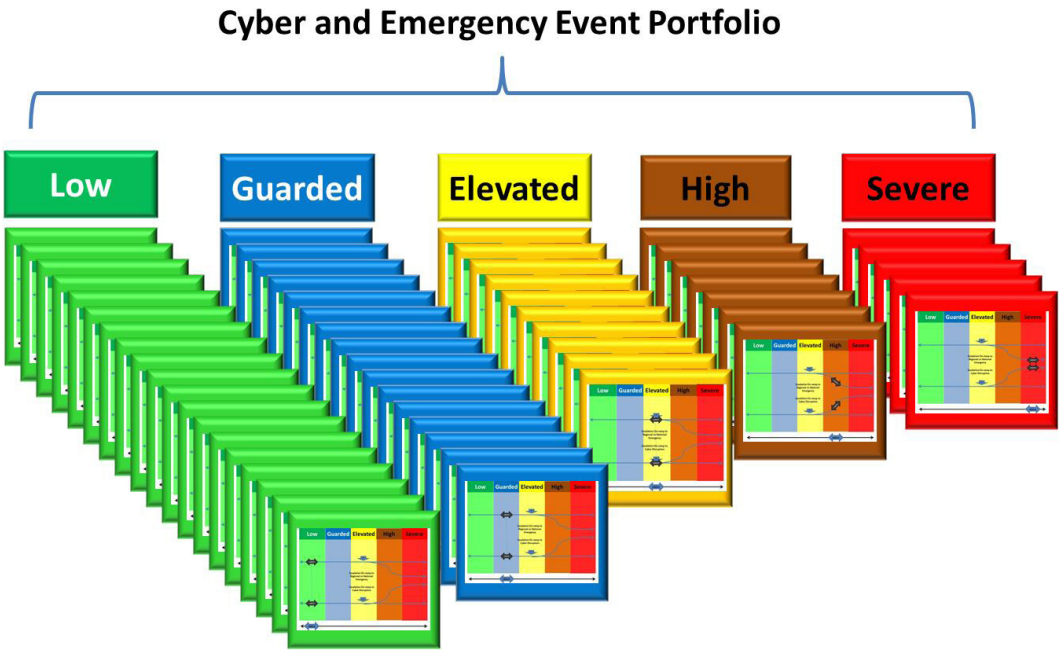
A cyber command center is a resource for state residents, groups, businesses and governments for the reporting, investigation and eventual prosecution of groups and individuals that commit cyber crimes. Members of the center are contributing partners in the State Cyber Disruption Response Plan. Cyber anomalies at any level that have a law enforcement nexus will be shared with the Cyber Command Center for possible investigation or analysis.

The state may have a national guard cyber unit that has capabilities for predicting, detecting, defending, mitigating and investigating cyber

disruptions. Those capabilities should be engaged at all threat levels particularly when a threat is first suspected to appear to more than a cyber incident.

In addition, a state may have a fusion center that provides cyber threat intelligence capabilities that will be employed by the state to predict and mitigate cyber disruption events. The fusion center is an essential member of the cyber disruption team and will help provide a common operating picture that will assist state police in investigating a cyber disruption event.

Ongoing threats should be monitored and continually evaluated throughout their lifecycle with a threat portfolio management system. Such a portfolio would show the current threat landscape as well as the ongoing classification and potentially reclassification of an event throughout its lifecycle.



Threat Portfolio

Training

State government must develop a **training** strategy. A training strategy will encompass every organization and every employee. Training is not just for the security professional. Every employee must understand security as a dimension of their role. In a cyber disruption incident, every employee has a part to play in keeping government going and the continuance of government services as government works its way through a crisis. The state government cyber force entails many roles from security professionals involved in forensics and incident management, to administrators supporting the application, hardware and devices, and networks. As well, all employees need to be trained on the use of alternative means for conducting business.

Potentially anyone in state government may be contacted by citizens and the media. Employees should be trained on how to respond to citizen and media inquiries during an event so that state government presents itself as competent and cohesive. Further, exercising a cyber disruption plan on a regular basis is critical to ensuring all individuals know what to do in the event their state experiences a significant cyber event that requires executing the Cyber Disruption Response Plan. Training must be practiced, and practiced frequently, to ensure the quality of execution is flawless.

Developing a thoughtful and well-coordinated response to a cyber disruption is essential to protecting critical infrastructure. However, preventing one from occurring is the priority. A key component of any prevention strategy is the deployment of expert personnel that are prepared with the know-how and the tools necessary to maintain a high level of threat awareness, the capabilities for quickly detecting and mitigating vulnerabilities, and minimizing the consequences of cyber disruptions.

The cyber incident and cyber disruption response teams must be well practiced experts in the use of operating discipline, supporting tools and necessary cross organization orchestration with all of the stakeholders described earlier in this report. Frequent practice and ongoing development of new kinds of scenarios will ensure everyone knows what to do in an emergency. Critical infrastructure owners and operators must train staff in cybersecurity skills, and exercise their teams regularly to protect their systems and respond to cyber disruptions that overcome defenses.

It is imperative that states develop a plan for training and exercising cybersecurity professionals who are responsible for the defense of the state's critical infrastructure.

☐ Training Plan

The following training plan lists recommended capabilities, each associated with a domain of cybersecurity that is essential to the protection of critical systems. The development of these capabilities within the state cyber incident and cyber disruption teams and partners will fulfill the training goal within a cyber disruption plan.

- ☐ Application Level Security
  - ☐ Known Software/Database Vulnerabilities (Java, SQL)
  - ☐ Web Application Security
  - ☐ Application Based Attacks (Buffer Overflow, SQL Injection)
- ☐ Hardware and Device Level Security
  - ☐ Vulnerabilities of Routers, Switches, Servers
  - ☐ Cryptography
  - ☐ Firewalls
- ☐ Network Level Security
  - ☐ OSI Model and Protocols
  - ☐ Network Architecture (LAN, Wireless)
  - ☐ Network Based Attacks (wireless intercept, IP spoofing)
- ☐ Disaster Recovery and Business Continuity
  - ☐ Business Impact Analysis
  - ☐ Business Continuity Planning
  - ☐ Interdependency
- ☐ Computer Forensics
  - ☐ Seizure Concepts
  - ☐ Incident Investigation
  - ☐ Digital Evidence and Electronic Discovery
- ☐ Physical Security
  - ☐ Risks, Threats and Countermeasures
  - ☐ Physical Intrusion Protection
  - ☐ Access Control
- ☐ Incident Management
  - ☐ Incident Command System
  - ☐ Roles and Responsibilities
  - ☐ Incident Reporting

Recommendations	
✓	Identify all partners from across government, industry and non-profits to build a network of stakeholders related to cyber disruption planning.
✓	Establish positive collaboration among various stakeholders now – well in advance of a cyber disruption. There should be frequent non-crisis interaction in order to develop the necessary trust relationships that will be fully exercised during the stress of a real crisis.
✓	Integrate cyber disruption planning with emergency management operations.
✓	Establish the necessary governance for a regional cyber disruption plan. Governance will clearly define lines of responsibility for advisory and decision making roles based on effects and types of cyber disruption events.
✓	Establish a priority for activities based on near-term, medium term and long term time lines.
✓	Establish a means for sharing ideas across regional cyber disruption initiatives in order to leverage the best practices and innovative approaches.
✓	Identity vulnerabilities in current infrastructures including computer networks.
✓	Develop a strategy for continuity of communications within government and with its external partners specifically addressing the loss of telecommunications including internet and wireless networks.
✓	Develop communication and coordination procedures to ensure timely and effective response in the event of a cyber disruption.
✓	Develop contingency plans, alternative action plans considering secondary effects of regional emergencies and secondary effects of cyber disruptions.
✓	Identify what resources can be brought to bear from across the cohort of partners based on scenarios and effects.
✓	Carefully examine supply chains, particularly those that are relied upon by all partners. If the supply chain is broken for one partner, that is most likely the circumstance for other partners.
✓	Insure backup communications networks are ready to launch and that such networks can sustain for some period of time. Over time that sustainability should be continually improved.

✓	Develop test plans for coordinating response across several or more infrastructures.
✓	Begin to identify tactical and medium term strategies for addressing loss of power and telecommunications. Consider developing regional and local power grids that are isolated from the internet and would provide dependable power in the case of a blackout or brownout. Such a regional grid would be developed under cross-jurisdictional collaborative.
✓	Develop, maintain and test a cross functional process flow that describes how stakeholders will interact at all threat levels. A starting point for this effort could be existing cross functional process flows for cyber incident management. Such a process could be scaled up to include all necessary players to deal with a cyber disruption.
✓	Incorporate resiliency measures into the enterprise portfolio for processes, systems, data and information assets, hardware, cloud services, shared services. Attribute the level of criticality for all IT assets.
✓	Incorporate resiliency requirements into every project, program and management initiative.

Key Questions

1. Is there appropriate support for creating, sustaining and maturing a cyber disruption response plan?
2. What messaging is required to gain the necessary support for creating, sustaining and maturing a cyber disruption response plan?
3. Who are key executive sponsors critical to the success of a cyber disruption response plan?
4. Who are key stakeholders and partners that should be included in a cyber security response plan network?
    a. What critical infrastructure providers should be included?
    b. What manufacturers and distributors should be included?
5. What threat sharing networks currently are in place at the national, regional and local levels?
    a. What are the predictive capabilities of these networks?
    b. How quickly are network members informed when on member has identified a cyber threat?
6. What backup communications capabilities are in place to maintain communication locally, regionally and nationally?
7. What are key assets and roles that must be available at the various stages of a cyber disruption event?
8. What are the priority assets and a backup/recovery strategy for these assets?
    a. Assets critical to continuity of government
    b. Assets critical to responding to emergencies and disasters
9. Do we have appropriate interoperability between cyber incident response and emergency management functions? Are key roles and resources mapped to a cross functional process that clearly describes how they will interact and be deployed at various threat levels?
10. When was the cyber incident and cyber disruption response plan last tested through a tabletop exercise?
11. How long will it take for our jurisdiction to restore the delivery of power, water, natural gas, internet, sewage treatment, transportation?
12. What training is currently in place for existing cyber security staff? What new training should be added to shore up capabilities to support a cyber disruption response plan?
13. What modifications should be made to the NASCIO cyber disruption checklist and the NASCIO cross functional process to adapt those resources to our circumstances?
14. Is our state currently using national frameworks for planning, implementing and testing capabilities for cyber disruption response planning?
    a. NIST
    b. FEMA

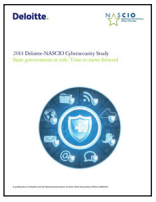
Appendix A – Contributors

NASCIO wishes to express its thanks to the following who were interviewed or contributed content during the research phase of this project.

- *Charlotte Allen, Executive Assistant, DTMB Cybersecurity & Infrastructure Protection, State of Michigan*
- *Glenn Archer, Deputy Director, National Fusion Center Association*
- *Erik Avakian, Chief Information Security Officer, Commonwealth of Pennsylvania*
- *David Bear, Senior Lead Marketing Manager, CenturyLink*
- *Valerie Bunsick, Marketing Associate, Field Marketing, Unisys*
- *John Byers, Former Chief Information Security Officer, State of Kansas*
- *Troy Campbell, National Fusion Center Association*
- *Sheri DeVaux, Security Manager, State of Connecticut*
- *Bill French, Director ITO, Commonwealth of Pennsylvania*
- *David Geick, Director of Security Services, State of Connecticut*
- *Pam Greenberg, Senior Fellow, National Conference of State Legislatures*
- *Don Heiman (retired), former Chief Information Technology Officer, State of Kansas Executive Branch and Legislative Branch*
- *Sam L. Hearn, Jr., Graphic Designer, AMR Management Services*
- *Deborah Henderson, Worldwide Program Director – DAMA-DMBOK www.dama.org, IEEE Professional Activities Board - IT Governance http://www.computer.org/portal/web/pab*
- *Kenny Holmes, CSSP, Account Executive, Palo Alto Networks*
- *Agnes Kirk, Chief Information Security Officer, State of Washington*
- *Emily Lane, Program and Brand Coordinator, NASCIO*
- *Chris Letterman, Chief Information Security Officer, State of Alaska*
- *Dan Lohrmann, Chief Strategist and Chief Security Officer, Security Mentor*
- *Major General Tim Lowenberg (retired), Former Adjutant General, State of Washington*
- *Daniel Mahoney, National Fusion Center Association*
- *Mark McChesney, Information Security Officer, Commonwealth of Kentucky*
- *Andris Ozols, NASCIO Special Advisor*
- *Meghan Penning, Membership and Communications Coordinator*
- *Richard Reasner, Director of Michigan Cyber Security, State of Michigan*
- *David J. Roberts, Senior Program Manager, IACP Technology Center, International Association of Chiefs of Police*
- *Doug Robinson, Executive Director, NASCIO*
- *Deborah A. Snyder, CISSP, CRISC, PMP, Deputy Chief Information Security Officer*
- *Elayne Starkey, Chief Security Officer,State of Delaware*
- *Lisa Thompson, Deputy Director, NASCIO*
- *Meredith Ward, Senior Policy Analyst, NASCIO*
- *Mike Watson, Chief Information Security Officer, Commonwealth of Virginia*

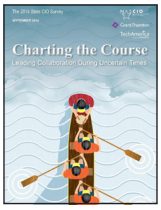
Appendix B – Resources for Further Study

NASCIO – www.nascio.org/publications



2014 Deloitte-NASCIO Cybersecurity Study - State governments at risk: Time to Move Forward October 2014

This study reports findings and analysis of a comprehensive survey of State Chief Information Security Officers (CISOs) conducted by NASCIO in partnership with Deloitte. The results of the 2014 Deloitte-NASCIO Cybersecurity Study confirm the growing importance of cybersecurity for states.



2014 State CIO Survey: Charting the Course September 2014

NASCIO, TechAmerica, and Grant Thornton LLP have collaborated for a fifth consecutive year to survey state government IT leaders on current issues, trends and perspectives

NASCIO 2014 Cybersecurity Awareness Resource Guide September 2014

For the 2014 observance of National Cyber Security Awareness Month, NASCIO has updated its Resource Guide for State Cybersecurity Awareness, Education, and Training Initiatives. The guide includes new information from our state members, who provided examples of state awareness programs and initiatives.

The States and FirstNet: An Early Look from the State CIOs June 2014

As states begin to plan for FirstNet, a nationwide high-speed wireless broadband network dedicated to public safety, they are developing divergent approaches to planning and varied strategies for engaging with local and federal partners. This research report is based on the results of a survey of State CIOs.

State CIO Top Ten Policy and Technology Priorities for 2014
November 2013

Each year NASCIO conducts a survey of the state CIOs to identify and prioritize the top policy and technology issues facing state government. The top ten priorities are identified and used as input to NASCIO's programs, planning for conference sessions, and publications.

NASCIO Cybersecurity Awareness Resource Guide September 2015

For the 2015 observance of National Cyber Security Awareness Month, NASCIO has updated its Resource Guide for State Cybersecurity Awareness, Education, and Training Initiatives. The guide includes new information from our state members, who provided examples of state awareness programs and initiatives.

Capitals in the Clouds Part V: Advice from the Trenches on Managing the Risk of Free File Sharing Cloud Services
April 2013

Cloud-based file sharing solutions have become very popular and certainly a growing and significant part of day-to-day computing. It is easy to see why these services are attractive to state government users after using them in many facets of their personal life. This brief helps to provide real experience from Commonwealth of Pennsylvania on free cloud services.

NASCIO Technology Awards
http://www.nascio.org/Awards/SIT

National Governors Association - Resource Center for State Cybersecurity
To help states address the consequences of the rapidly evolving and expanding technological threats now faced by law enforcement agencies, public works and energy agencies, private financial and communications sectors and the general public, the National Governors Association (NGA) launched a Resource Center for State Cybersecurity (Resource Center).
www.nga.org/cms/statecyber

Releases

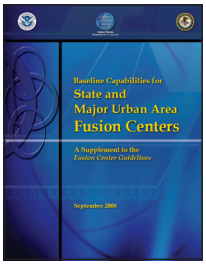
- *Fusion Centers Play Leading Role In Promoting Cybersecurity*
- *Cybersecurity Workforce Key To Combating Threats*
- *Governors Focus on State Cybersecurity and State-Federal Coordination*
- *Governors O'Malley and Snyder to Lead NGA Resource Center on Cybersecurity*

Resources

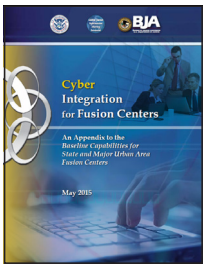
- *Federal Cybersecurity Programs: A Resource Guide*
- *Act and Adjust: A Call to Action for Governors for Cybersecurity*
- *State Roles in Enhancing the Cybersecurity of Energy Systems and Infrastructure*

National Fusion Center Association (NFCA).
The mission of the NFCA is to represent the interests of state and major urban area fusion centers, as well as associated interests of states, tribal nations, and units of local government, in order to promote the development and sustainment of fusion centers to enhance public safety; encourage effective, efficient, ethical, lawful, and professional intelligence and information sharing; and prevent and reduce the harmful effects of crime and terrorism on victims, individuals, and communities.
www.nfcausa.org

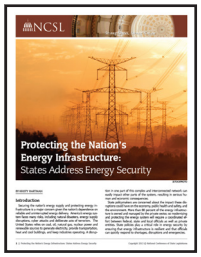
- ***Addendum to the Baseline Capabilities***
  This document identifies the baseline capabilities for fusion centers and the operational standards necessary to achieve each of the capabilities. It is an addendum to the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative's (Global) Fusion Center Guidelines, which provide guidance to ensure that fusion centers are established and operated consistently across the country. Using the Fusion Center Guidelines, as well as identified best practices, federal, state, and local officials identified the capabilities and standards necessary for a fusion center to be considered capable of performing basic functions.
  https://www.it.ojp.gov/documents/d/baseline%20capabilities%20for%20state%20and%20major%20urban%20area%20fusion%20centers.pdf



- ***Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers***
  This document identifies recommended actions and guidance for state and major urban area fusion centers (fusion centers) to integrate information technology, cybersecurity, and cybercrime1 prevention (cyber) intelligence and analytic capabilities. Development of these capabilities will inform local, state, and national detection, mitigation, response, recovery, investigation, and criminal prosecution activities that support and maintain the United States' cybersecurity. This document is an appendix to the Global Justice
  Information Sharing Initiative's (Global) Baseline Capabilities for State and Major Urban Area Fusion Centers (Baseline Capabilities).
  http://it.ojp.gov/GIST/178/Cyber-Integration-for-Fusion-Centers--An-Appendix-to-the-Baseline-Capabilities-for-State-and-Major-Urban-Area-Fusion-Centers



National Conference of State Legislatures



Protecting the Nation's Energy Infrastructure: States Address Energy Security
- *Presents a list of relevant state legislation regarding infrastructure protection*

http://www.ncsl.org/documents/energy/EnergySecurityFinal-10-13.pdf

Data Breach legislation
http://www.ncsl.org/research/telecommunications-and-information-technology/2014-security-breach-legislation.aspx

Federal Resources

PRESIDENTIAL POLICY DIRECTIVE/PPD-8*, March 30, 2011,*
http://www.dhs.gov/presidential-policy-directive-8-national-preparedness

The purpose of Presidential Policy Directive (PPD-8) on national preparedness was to establish a foundation that could be adapted to and utilized by stakeholders at all public and private levels. PPD-8 essentially replaced Homeland Security Policy Directive (HSPD-8)

Executive Order -- Improving Critical Infrastructure Cybersecurity, February 12, 2013
https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Presidential Policy Directive - PPD21- Critical Infrastructure Security and Resilience,
February 12, 2013
https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Federal Emergency Management Agency (FEMA)
www.fema.gov

- ***National Preparedness Goal*** *(First Edition), FEMA, September 1, 2011,*

  The National Preparedness Goal organizes the core capabilities into the five mission areas which have been modified and supplemented by as sixth category for the NASCIO proposed disruption mission areas.

- ***National Disaster Recovery Framework****, FEMA, September, 2011, National Disaster Recovery Framework*

  The National Disaster Recovery Framework is a guide that enables effective recovery support to disaster-impacted States, Tribes, Territorial and local jurisdictions. It provides a flexible structure that enables disaster recovery managers to operate in a unified and collaborative manner. It is one of five frameworks

National Response Framework *(Second Edition), Homeland Security, May 2013*
https://www.fema.gov/media-library/assets/documents/32230?id=7371

The second edition of the National Response Framework (NRF), updated in 2013, provides context for how the whole community works together and how response efforts relate to other parts of national preparedness. It is one of the five documents in a suite of National Planning Frameworks. Each Framework covers one preparedness mission area: Prevention, Protection, Mitigation, Response or Recovery.

- *National Prevention Framework, Homeland Security, May 2013*
http://www.fema.gov/national-prevention-framework
- *National Protection Framework, Homeland Security, July 2014*
http://www.fema.gov/media-library/assets/documents/97350
- *National Mitigation Framework, Homeland Security, May 2013*
http://www.fema.gov/national-mitigation-framework
- *National Response Framework, Homeland Security, May 2013*
http://www.fema.gov/national-response-framework
- *National Recovery Framework, Homeland Security, September 2011*
http://www.fema.gov/national-disaster-recovery-framework-0

National Institute of Standards and Technology
www.nist.gov

- ***Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0***,

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. It directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure.
http://www.nist.gov/cyberframework/

IACP Law Enforcement Cyber Center
www.iacp.org/LawEnforcementCyberCenter

The Law Enforcement Cyber Center is an online portal that is designed to provide law enforcement officials—chiefs, investigators, line officers, and prosecutors—with comprehensive information and practical resources in preventing, investigating, mitigating, and responding to cybercrime and cyber-enabled threats. The Center addresses cybercrime investigation, digital evidence collection and management, and information systems security.

FBI- Cyber Shield Alliance
www.iacpcybercenter.org/resource-center/fbi-cyber-shield-alliance/

> *Cyber Shield Alliance (CSA) is an FBI cyber security partnership initiative developed by law enforcement for law enforcement to proactively defend and counter cyber threats against law enforcement networks and critical technologies. CSA encourages law enforcement participation as a force multiplier in defending our national security, while equipping agencies with the training and tools to optimize and defend their own law enforcement networks.*

Multi-State Information Sharing & Analysis Center (MS-ISAC)
www.msisac.cisecurity.org/

> *The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial (SLTT) governments. The MS-ISAC 24x7 cybersecurity operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.*

National White Collar Crime Center
www.nw3c.org/

> *For more than three decades, NW3C has worked to support the efforts of state and local law enforcement to prevent, investigate and prosecute economic and high-tech crime. Today, NW3C continues to strengthen this mission by staying current with the technological innovations of the digital age to keep law enforcement up-to-date.*

Regional Resources

Houston Regional Catastrophic Preparedness Initiative
Cyber Disruption Readiness Assessment Tool
This is a resource for evaluating cyber disruption readiness. It is openly available for conducting an assessment for state and local governments.
www.cyberdisruptionplanning.com

An overview of the initiative is available at:
https://www.preparingtexas.org/Resources/documents/2014%20TEMC/Houston%20Regional%20Catastropic%20Preparedness.pdf

***New England Regional Catastrophic Coordination Plan, Cyber Disruption Response Annex*, NERCPI, Prepared by URS Corporation, January 2012**

The Cyber Disruption Response Annex (CDRA) is a subset of the Regional Catastrophic Coordination Plan (RCCP), a planning effort of the Regional Catastrophic Planning Team (RCPT) that facilitates the coordination of all-hazards preparedness, situational awareness, response, and recovery activities of the States of New Hampshire and Rhode Island, the Commonwealth of Massachusetts, and the Urban Area Security Initiative cities of Boston and Providence—collectively known as the Regional Catastrophic Planning Area (RCPA). The CDRA fosters relationships and mutual understanding of institutional missions and capabilities to ultimately facilitate coordination for cyber-related regional catastrophic incidents.

Appendix C – Emergency Support Functions (ESFs)

The ESFs provide the structure for coordinating interagency support for a state response to an emergency or disaster. They are mechanisms for grouping functions most frequently used to provide state and federal support to local jurisdictions and tribes for proclaimed states of emergencies.

ESF	Scope of Responsibilities
ESF 1 – Transportation	Aviation/airspace management and control Transportation safety Restoration/recovery of transportation infrastructure Movement restrictions Damage and impact assessment
ESF 2 – Communication, Information and Warning Systems	Coordination with telecommunications and information technology industries Restoration and repair of telecommunications infrastructure Protection, restoration, and sustainment of national cyber and information technology resources Oversight of communications within the Federal incident management and response structures
ESF 3 – Public Works and Engineering	Infrastructure protection and emergency repair Infrastructure restoration Engineering services and construction management Emergency contracting support for life-saving/sustaining services
ESF 4 – Firefighting	Coordination of Federal firefighting activities Support to wildland, rural, and urban firefighting operations

ESF 5 – Emergency Management	Coordination of incident management and response efforts Issuance of mission assignments Resource and human capital Incident action planning Financial management
ESF 6 – Mass Care, Emergency Assistance, Housing and Human Services	Mass care Emergency assistance Disaster housing Human services
ESF 7 – Logistics Management and Resource Support	Comprehensive, national incident logistics planning, management, and sustainment capability Resource support (facility space, office equipment and supplies, contracting services, etc.)
ESF 8 – Public Health and Medical Services	Public health Medical Mental health services Mass fatality management
ESF 9 – Search and Rescue	Life-saving assistance Search and rescue operations
ESF 10 – Oil and Hazardous Materials Response	Oil and hazardous materials (chemical, biological, radiological, etc.) response Environmental short- and long-term cleanup

ESF 11 – Agriculture and Natural Resources	Nutrition assistance Animal and plant disease and pest responses Food safety and security Natural and cultural resources and historic properties protection and restoration Safety and well-being of household pets and service animals
ESF 12 – Energy	Energy infrastructure assessment, repair, and restoration Energy industry utilities coordination Energy forecast
ESF 13 – Public Safety and Security	Facility and resource security Security planning and technical resource assistance Public safety and security support Support to access, traffic, and crowd control
ESF 14 – Long-Term Community Recovery	Social and economic community impact assessment Long-term community recovery assistance to States, local governments, and the private sector analysis and review of mitigation program implementation
ESF 15 – External Affairs	Emergency public information and protective action guidance Media and community relations Congressional and international affairs Tribal and insular affairs
ESF 20 – Defense Support to Civil Authorities	Coordination with Dept. of Defense for military resources Coordination with FEMA Region X Defense Coordinating Office Resource tasking to Washington National Guard and State Guard

(Endnotes)

1 Chase, L., "Resiliency Planning and Continuity of Operations: Beyond Disaster Planning." chapter 13 *CIO Leadership for Cities and Counties – Emerging Trends and Practices*. 2009. Public Technology Institute. Washington, D.C. ISBN 1-4392-4078-7.

2 Bussey, J., "How the Sony Breach Changes Cybersecurity" *The Wall Street Journal*, Feb. 9, 2015. Web. Retrieved on June 6, 2015, from http://www.wsj.com/articles/how-the-sony-data-breach-signals-a-paradigm-shift-in-cybersecurity-1423540851

3 Lee, T.B., "The Sony hack: how it happened, who is responsible, and what we've learned." *Vox Technology,* December17, 2014. Web. Retrieved on June 6, 2015, from http://www.vox.com/2014/12/14/7387945/sony-hack-explained.

4 Sidel, R., "Home Depot's 56 Million Card Breach Bigger Than Target's." *The Wall Street Journal*, Sept. 18, 2014. Web. Retrieved on June 6, 2015, from http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571

5 Bateman, T., "Millions of US government workers hit by data breach." *The BBC*, June 5, 2015. Web. Retrieved on June 6, 2015, from http://www.bbc.com/news/world-us-canada-33017310.

6 Lohrmann, D., , "2014: The year cyber danger doubled." Government Technology, *Lohrmann on Cybersecurity & Infrastructure*. December 21, 2014. Retrieved on June 15, 2015, from http://www.govtech.com/blogs/lohrmann-on-cybersecurity/2014-The-year-cyber-danger-doubled.html.

7 *Framework for Improving Critical Infrastructure Cybersecurity*, v 1.0, February 12, 2014. National Institute of Standards and Technology. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

8 *2015 National Preparedness Report*, March 30, 2015. US Department of Homeland Security, Federal Emergency Management Agency. Retrieved from https://www.fema.gov/national-preparedness-report.
9 The National Preparedness Goal. For more information see http://www.fema.gov/national-preparedness-goal.

10 See FEMA National Planning Frameworks. http://www.fema.gov/national-planning-frameworks

11 FEMA *National Protection Framework*, July 2014. p.11. Retrieved from http://www.fema.gov/national-planning-frameworks.

12 *The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation*. Strategic National Risk Assessment. December 2011. Retrieved on June 10, 2015, from http://www.dhs.gov/strategic-national-risk-assessment-snra.

13 See Michigan Cyber Disruption Response Strategy - www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf
See New England

14 NIST Cybersecurity Framework. http://www.nist.gov/cyberframework/.

15 Definition derived from the National Cyber Incident Response Plan, Interim Version, dated September 2010.

16 Adapted from the NIPP Risk Management Framework. U.S. Department of Homeland Security (2009). National Infrastructure Protection Plan (NIPP). Washington, DC:
U.S. Department of Homeland Security. p.27. Available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

SECTION 02

CYBER DISRUPTION RESPONSE CHECKLIST

NASCIO Representing Chief Information Officers of the States

Guidance for Coordinated and Integrated Cybersecurity Disruption Response Planning: Essential Elements

The following worksheet is intended to list essential elements of any coordinated or integrated cybersecurity disruption plan. We encourage state cybersecurity teams to utilize this worksheet as a starting point for a discussion regarding governance, organization, and planning essential elements of risk reduction and response to cyber disruptions. We're using this worksheet to also collect your ideas and suggestions for additional content to be included here as well as in our more comprehensive guidance on cyber disruption response planning.

It is important to keep in mind that cybersecurity disruptions are:

- of a magnitude that requires a much more rigorous and sustained response than more typical or routine cyber incidents, and
- may require coordination and collaboration among a wider range of responders, partners, frameworks and plans with cyber elements.

A significant cyber disruption event is defined "as an event or effects from events that are likely to cause, or are 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 that provide direct information technology services or enabling and support capabilities for other services; and/or threaten public safety, undermine public confidence, have a negative effect on the state economy, or diminish the security posture of the state.[1]"

1 Definition derived from the National Cyber Incident Response Plan, Interim Version, dated September 2010.

Essential Elements

Checklist Subject Areas:

- ☐ **Authority, Governance and Decision Points**
  - ☐ **Organization, Roles and Processes**
  - ☐ **Capability and Risk Assessment**
- ☐ **Implementation, Management and Operations**
  - ☐ **Communications**
  - ☐ **Response and Recovery**
  - ☐ **Evaluation and Improvement**
- ☐ **Plan Maintenance, Corrective Action and Updates**
  - ☐ **Training and Exercising**
  - ☐ **Form for Feedback and Continual Improvement**

Note: please identify and document any missing element categories or elements you believe to be essential to adequate cyber disruption planning and send recommendations for any such updates to the project director.

☐ **Authority, Governance and Decision Points**

Established Authority—What is the basis for the authority for creating a cyber disruption response plan or plans, including the scope and limits of authority? Governance should be well established and operating well in advance of any cyber disruption event.

☐ *State Statutes or Regulations* ☐ *State Executive Orders & Directives* ☐ *Formal Agreements Among Governance Partners*	☐ *Federal law* ☐ *Federal Regulations* ☐ *Federal Executive Orders* ☐ *National or Collaborative Standard Setting or Analytic Entities* ☐ *Other* _____

Who is involved in cyber disruption planning and have they been consulted and included? Outline the responsible party(ies) from, and any decision rights for, the following entities:

- ☐ *Office of the Governor*
- ☐ *State CIOs office, and CISO*
- ☐ *Homeland Security*
- ☐ *Emergency Management Agencies*
- ☐ *Public Safety, incl. State Police*
- ☐ *Fusion Centers*
- ☐ *National Guard*
- ☐ *Other State Agencies / Health, Transportation, Education,*
- ☐ *Regional Partners (other states, tribes, nations, and territories)*
- ☐ *Utilities, Private Sector, Industry and Service Providers (e.g. Health)*
- ☐ *Intergovernmental Agencies (Federal and local)*
- ☐ *Other* _____

Establish decision points mapped to the lifecycle of an event including determining threat level, action plans and resource allocation.

- ☐ How do we classify an event and its severity?
- ☐ What are the critical decision points for each classification?
- ☐ How are decision points staged, coordinated and / or integrated
- ☐ How is information shared, tracked and managed?
- ☐ Who is responsible for escalating or deescalate a cyber event?
- ☐ Who has lead responsibility at each point?
- ☐ Who has supportive responsibility at each point?
- ☐ Who is responsible for after action, evaluation, reports, and improvements?
- ☐ Other decision points _____

☐ Organization, Roles and Processes

Roles, Functions and Responsibilities utilizing the Governance section above, what are the roles, functions and responsibilities for the Cyber Disruption Team during an event? Consider including primary functions and responsibilities, support functions and roles, and information dissemination recommendations and requirements. What additional roles should be included?

☐ *Governor's staff* ☐ *CIO staff* ☐ *CISO staff* ☐ *Emergency Management staff* ☐ *State Police* ☐ *National Guard* ☐ *Fusion Center*	☐ *Homeland Security* ☐ *Local Governments* ☐ *Public Information & Communications* ☐ *Selected private sector partners, including industries and services* ☐ *Other* _____ _____

Function and Process Prioritization and Coordination—Overlay the functions, roles and responsibilities map with the defined functions, processes and operating procedures among all listed members of the organization listed in cyber disruption governance. Consider mapping them for the following: Predict, Prevent, Detect, Analysis, Response, Recovery, Evaluation, and Enterprise Maintenance and Improvements. Consider indicating priorities

☐ Preparedness Activities – Resiliency, Capability and Risk Assessment

Capability and Risk Reduction Elements —Much of the capability and risk assessment may have been done for physical infrastructure, but has it been done for cyber infrastructure and services? Consider whether your team has conducted a systematic capability or risk assessment or fully reviewed and identified the following in a collaborative environment. What should be added?

In general, preparedness activities should include the following:

- ☐ Identify threats and vulnerabilities to IT networks with respect to emergency management objectives and priorities
- ☐ Identify mitigations (e.g. plans, procedures, hardening measures, etc.) for threats and vulnerabilities
- ☐ Develop communications means and methodologies to enable intra- and extra-jurisdictional transactions
- ☐ Develop plans and procedures to address specific disruptions
- ☐ When necessary and possible, communicate with other jurisdictional RCPA CDT
  - representatives to exchange best practices

Detailed Activities:

- ☐ Conduct short and long-term cyber disruption needs and prognosis analysis;
- ☐ Conduct a formal resiliency, capability and risk assessment
- ☐ Create written backup and recovery policies and procedures

- ☐ Data and Information Assets
  - ☐ Inventory data and information assets;
  - ☐ Classify and value data and information assets;
  - ☐ Use classification and value assessment to determine data protection measures;
  - ☐ Develop priorities for data availability;
  - ☐ Identify risks to data and information assets;
  - ☐ Develop backup and recovery solutions for critical data;
  - ☐ Identify and assess any privacy risks and mediation requirements;

- ☐ Software, systems and infrastructure;
  - ☐ Identify critical infrastructure and key resources;
  - ☐ Maintain an inventory of all software;
  - ☐ Create procedures for surfacing software that is beyond warranties and service level agreements;
  - ☐ Establish operating procedures for evaluating warranties and service level agreements in a timely fashion to avoid loss of supplier support;
  - ☐ Establish meta data to maintained for all software including criticality and co-dependency with other systems and software;
  - ☐ Determine what systems and services must survive a cyber disruption;
  - ☐ Develop resiliency plans for these systems and services;
  - ☐ Create necessary backup sites as necessary to maintain systems and processes that must survive a disaster;
  - ☐ Identify threats to the IT subject infrastructure;
  - ☐ Identify vulnerabilities of the target infrastructure to the identified threats;
  - ☐ Identify consequences of a successful attack on the IT subject infrastructure;
  - ☐ Identify risk to the IT subject infrastructure based on the aforementioned factors;
  - ☐ Identify means of reducing risk to IT subject infrastructure;
  - ☐ Identify resources available to mitigate risk;
  - ☐ Implement virtualization and replication technologies and best practices for ensuring continuity of government business;

- ☐ Workforce
  - ☐ Identify all personnel that are in critical roles for managing a cyber event for all threat levels;
  - ☐ Identify all roles and personnel required to keep critical systems and processes running during a crisis;
  - ☐ Determine all duties of critical personnel including potential roles during local emergencies such as volunteer EMTs, firefighters, public safety roles, that could affect their availability to participate as a member of the cyber disruption response team;
  - ☐ Establish emergency hiring and contracting procedures;
  - ☐ Establish the necessary backup of critical roles; at a minimum critical roles should have primary and secondary personnel named;
  - ☐ Document organizational charts in both digital and paper media;
  - ☐ Establish necessary backup for critical equipment including network operations, critical systems, and backup power generation;

- ☐ Develop a business continuity plan that includes business impact analysis, recovery strategies and procedures, continuity of business operations strategies and procedures, backup staffing strategies and procedures;
- ☐ Develop cross-training strategies and procedures;
- ☐ Create staff knowledge and skill set inventories;
- ☐ Document manual procedures using both digital and paper records management strategies;
- ☐ Develop strategies for workforce to be able to work remote in case of public health events such as pandemic influenza;

☐ Access to systems and applications
- ☐ Determine remote access needs during a cyber disruptions;
- ☐ Identify critical systems that can only be accessed on-premise;
- ☐ Evaluate access strategies including remote application access which may be exercised in an emergency situation;
- ☐ Verify number of licenses is adequate to keep government operations running if workers need to work from remote sites;
- ☐ Evaluate virtual private networks and the potential for increasing capacity during a cyber disruption;

☐ Physical access to facilities
- ☐ Implement physical access controls;
- ☐ Implement visitor sign in /out policy;
- ☐ Implement key card access to critical areas;

☐ Equipment
- ☐ Inventory and classify all equipment regarding criticality;
- ☐ Ensure there is 24/7/4 service level support with manufacturer(s) or service vendor(s) for servers, desktops, laptops, and other technologies required to support critical business processes, systems, and applications;
- ☐ Establish and maintain an inventory of replacement desktops, laptops and spare parts;
- ☐ Identify minimum hardware and software requirements to support operations, critical business processes and normal operations;
- ☐ Identify suppliers that can provide temporary equipment during cyber disruptions;
- ☐ Establish backup procedures using secondary sources for equipment;
- ☐ Establish backup procedures that involve manual procedures if equipment is damaged or destroyed and secondary sources are not available;
- ☐ Establish emergency purchasing procedures;
- ☐ Evaluate lease agreements regarding backup equipment;

☐ Network / Internet / Cloud services
- ☐ Develop operational procedures for critical business systems and processes in the event of loss of internet connectivity;
- ☐ Develop operational procedures for non-critical business systems and processes in event of loss of internet connectivity;
- ☐ Determine the how long operations can sustain a loss of internet and network services before critical systems and processes are severely affected;

- ☐ Develop failover telecommunications capabilities;
- ☐ Develop backup procedures for using for routing internet traffic through regional partner(s) over Wide Area Networks (WAN);
- ☐ Develop back procedures for automatic failover to secondary internet service provider(s);
- ☐ Ensure secondary internet provider(s) have the necessary capacity to support critical business systems and processes, and anticipated access during a cyber disruption;
- ☐ Establish protocols and procedures for managing planned and unplanned outages experienced by the internet service provider(s) and cloud service provider(s);
- ☐ Establish priority Service Level Agreement(s) with internet service providers
- ☐ Establish priority Service Level Agreement(s) with cloud services providers
- ☐ Determine how long a hot/warm site can remain viable as a backup during a cyber disruption event
- ☐ Develop procedures for trading out network equipment that may be damaged during a cyber disruption event
- ☐ Develop a list of critical network components that must be kept on hand for swapping out equipment during a cyber disruption event
- ☐ Develop protocols and procedures for providing backup access to critical services by citizens

- ☐ Utilities (electrical distribution, water distribution, sewer, transportation services)
  - ☐ Create operational procedures for dealing with the loss of critical utilities and infrastructure services
    - ☐ electrical power
    - ☐ water
    - ☐ sewer
    - ☐ transportation
    - ☐ telecommunications
    - ☐ radio
  - ☐ Determine how long operations can sustain a loss of critical utilities and infrastructure services
    - ☐ electrical power
    - ☐ water
    - ☐ sewer
    - ☐ transportation
    - ☐ telecommunications
    - ☐ radio
  - ☐ Electrical power
    - ☐ Purchase and install the necessary backup power generation to maintain critical business processes and systems during a power outage;
    - ☐ Determine how long facilities can continue to operate on backup generators including reserve fuel supplies and supply lines;
    - ☐ Develop strategies for reducing the load to increase run time on generators;
    - ☐ Evaluate contracts with fuel providers;
    - ☐ Ensure service level agreements with fuel providers meets the needs anticipated during a cyber disruption event;
    - ☐ Ensure there is automated failover to backup generators;
    - ☐ Maintain a supply of replacement parts, supplies and maintenance tools for backup generators;

- ☐ Maintain paper and electronic records related to backup power generation equipment including:
  - make and model of the generator
  - wattage output
  - location(s)
  - fuel type
  - fuel storage tanks
- ☐ Maintain records on reserve fuel;
- ☐ Recycle fuel as necessary;
- ☐ Document runtime limits on generators as a function of output wattage;
- ☐ Establish physical security in and around generators, fuel tanks and pipelines;
- ☐ Test circuits and outlets serviced by the generators
- ☐ Ensure proper power connections to external power generators is installed; It may be necessary to backup the backup generators with mobile units;
- ☐ Ensure generators have proper schedule maintenance and testing;
- ☐ Ensure all critical equipment is on uninterruptable power supplies (UPS) and that power is properly regulated;
- ☐ Ensure backup batteries are charged;
- ☐ Maintain an inventory of backup batteries;

- ☐ Business processes
  - ☐ Identify business processes that are critical during a cyber disruption or emergency
  - ☐ Develop workaround for continuing critical business processes without supporting staff and technology;
  - ☐ Develop manual workaround for critical processes;

- ☐ Identify and incorporate relevant cyber elements from existing state overall or IT plans, explicit state IT security plans, emergency management annexes, homeland security plans, disaster recovery plans, industry and service related plans
- ☐ Develop an operational and strategic coordination and integration framework for existing plans or frameworks
- ☐ Other_____

- ☐ Utilize the elements above as a basis for developing a risk management strategy taking into account the risk priorities and resources available.

☐ **Implementation, Management and Operations for Cyber Disruption Response Plans**

- ☐ Establish a timeline for delivering key components of a cyber disruption response plan:
  - ☐ *the organization,*
  - ☐ *process,*
  - ☐ *system, process and data inventories,*
  - ☐ *risk assessments,*
  - ☐ *mitigation plans,*
  - ☐ *roles and responsibilities*
- ☐ Identify unique State Issues, Opportunities and how they influence short and long range next steps

- ☐ Develop further characterization of implementation steps:
  - **Priority**, applicable to all states, top priority
  - **Desirable**, depending on state characteristics may be in short term or long range. e.g. Power applies to all states, hurricanes more of a risk for others
  - **Future**, can't address now, but should be added in a future versions

- ☐ Develop an Implementation, Management and Operations process plan
- ☐ Develop a calendar for implementation

☐ Communication

Key Response Communication—coordinating among key actors is integral to operational coordination to deal with primary and secondary effects, and cross-jurisdictional partnering. States should establish the following:

- ☐ Develop a communications protocol integrated with cross-functional process flows, potentially through an existing or planned joint information center that will be activated for the duration of a cyber disruption.
- ☐ Establish ongoing communication across the security and emergency management ecosystem / communities through periodic meetings and conference calls. Formation of cyber disruption response teams should not be reactive. The teams should always be in place, evaluating, communicating, acting preemptively as well as reactively.
- ☐ Establish alternative means for enabling communications in case certain technologies (power supplies, fuel for emergency power, e-mail, phone, public safety communications) are unavailable.
- ☐ Public Information Plan—develop communication and education to raise awareness across state agencies, external partners and the public regarding the current threat landscape, the interdependencies of infrastructures, the necessity of developing effective strategies for cyber disruption response plans and responsibility for individual actions to be taken.
- ☐ Establish contact lists for:
  - ☐ Internet service providers
  - ☐ Critical systems support and backup
  - ☐ Mutual aid agreements

☐ Response and Recovery

Reactive and Pro-Active Responses A key component of any strategy is the deployment of qualified personnel with subject matter expertise that are prepared with the know-how and the tools necessary to maintain a high level of threat awareness, quickly detect and mitigate vulnerabilities, and minimize the consequences of cyber disruptions. Another aspect is the balance among pro-active and maintenance and response strategies such as trustworthy systems and processes, defensive and adaptive systems, predictive and proactive defenses, and cyber-analytics.

In general response activities should include the following.

- ☐ Monitor events and share and collect information among or between cyber disruption response teams that may indicate the development of a regional catastrophic cyber incident
- ☐ Provide other jurisdictional cyber disruption response team representatives with situational awareness and assistance during a catastrophic incident as necessary and possible

- ☐ Provide situational awareness and subject-matter expertise and solutions for an Incident/Unified Commander and his/her General Staff during a response,
- ☐ Coordinate IT-related intra- and inter-jurisdictional response activities pursuant to any regional incident action plans
- ☐ Coordinate with Incident/Regional Command staff and state Emergency Support Function 2 (ESF-2) to procure critical cyber-related resources

Pro-Active Analytics Capabilities

- ☐ Establish operating capabilities and operating discipline for advanced predictive analytics that will move state government more toward pre-emptive, preventative as possible.
- ☐ Identify strategic partners that can provide predictive intelligence on emerging threats

Recovery—entails the restoration of normal operations. This can involve migrating from the cold, warm or hot site back to on premise systems or primary cloud services.

In general the recovery activities should include the following.

- ☐ Work with affected system and service owners and managers to determine resources and sequencing needed to restore operations to a normal state;
- ☐ Track restoration efforts and provide information to the emergency management team (EMT) regarding estimated and actual time to full restoration;
- ☐ Establish procedures and protocol for migrating back to primary systems, network and normal operations when coming out of a cyber disruption event;
- ☐ Establish recovery time objectives (RTOs) for
  - ☐ equipment,
  - ☐ networks,
  - ☐ critical business processes and systems,
  - ☐ accessibility to critical data
  - ☐ citizen services

☐ Evaluation and Improvement

Research Lessons Learned—What learnings can be gained from previous events and event response; and other jurisdictions?

- ☐ Conduct internal and external cyber disruption team (CDT) after action reviews and assessments to obtain lessons learned following an cyber disruption

☐ **Plan Maintenance, Corrective Action and Updates**

Based on the performance results from actual events, tabletop exercises, drills and practice, modify the cyber disruption response plan to take account of lessons learned, process steps that need to be improved, potential new roles, and the addition of new technologies.

- ☐ Participants, including changing roles and inclusion of new stakeholders
- ☐ Process descriptions
- ☐ Inclusion of lessons learned, engagement of new issues and adoption of new solutions
- ☐ Decision points and calendar
- ☐ Lessons learned; Improvements; Ongoing enhancement of the cyber disruption response plan

Analysis of Mitigation Strategies—What feedback from past events can be used to modify / improve mitigation strategies? i.e., continual improvement

- ☐ _____
- ☐ _____

Analysis of Real and Potential ROI—Economic evaluation of cyber response strategies to demonstrate real and potential cost avoidance related to loss prevention, saving of lives, saving of assets and infrastructure.

- ☐ _____
- ☐ _____

☐ Training and Exercising

- ☐ **Training**—Determine training requirements are necessary for developing team capabilities to anticipate, prevent, respond to and recover from a cyber disruption event.
- ☐ **Exercise**—Define what exercises should be run to test and improve cyber disruption response plans. Determine how often should these exercises be run.
- ☐ **Test the activation** of hot/warm sites on a periodic basis
- ☐ **Test the performance** of critical services and functions using backup equipment and cloud services
- ☐ **Test backup and recovery** policies and procedures on an established schedule (annual, six months, quarterly)
- ☐ **Test backup power sources** including generators and battery backups
- ☐ **Participants** – Identify who should participate and how frequently

For more information or to suggest additions to this guide, contact the NASCIO Project Director Eric Sweden.

SECTION 03

CYBER DISRUPTION RESPONSE CROSS-FUNCTIONALITY REPORT

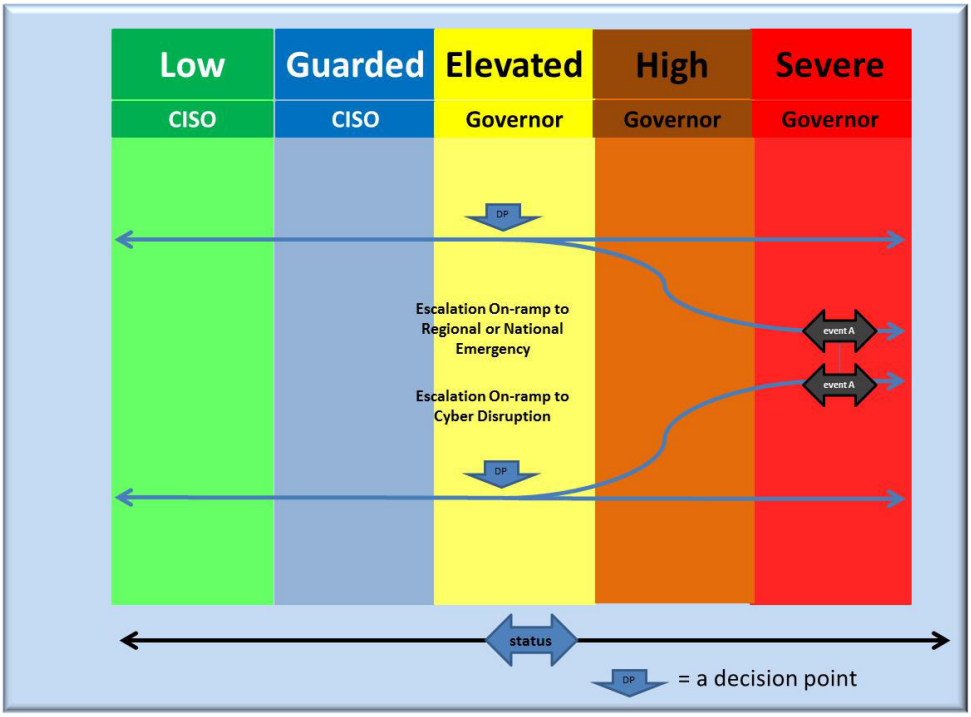
Cyber Disruption Response Plan Roles and Responsibilities

During a cybersecurity disruption, state government will need to work with federal, state, and local agencies and organizations; K-12; higher education; and private industry to respond to a cyber disruption, resolve the disruption and address any secondary effects that arise from a cybersecurity disruption, man made disaster, or natural disaster. The following will provide a *proforma* set of roles, responsibilities and cross-functional process for coordinating / orchestrating organizations and resources during a cybersecurity event that first surfaces as a cyber event and which escalates to be categorized as a cyber disruption. States and territories should adapt this guidance to their specific circumstances, roles and responsibilities. The major reference that provided a model for this component report in NASCIO's cyber disruption response planning guidance is the *Commonwealth of Pennsylvania Cyber Security Incident Response Plan*.

A cyber disruption event can be expected to initially surface as a cyber incident or as an emergency management incident. The general term that may be used by state government is "an event." Any event must be continually monitored in order to understand potential escalation of such an event to a cyber disruption or significant emergency management event. For example, an event may occur that initially surfaces as what may initially appear to be a cyber incident. It is with a comprehensive view of all incidents that are currently active that may cause the cyber disruption team to identify a pattern of complex incidents that indicate something of greater magnitude than a single occurrence cyber incident.

A second example is an emergency event that first surfaces as a disruption in some key infrastructure or the delivery of some utility such as distributed electrical power, water, natural gas, interruption in waste water treatment, loss of telecommunications or internet services, interruption in wireless service, or radio communications. As the event is being evaluated by emergency management, it may be discovered that the underlying cause is a cyber disruption.

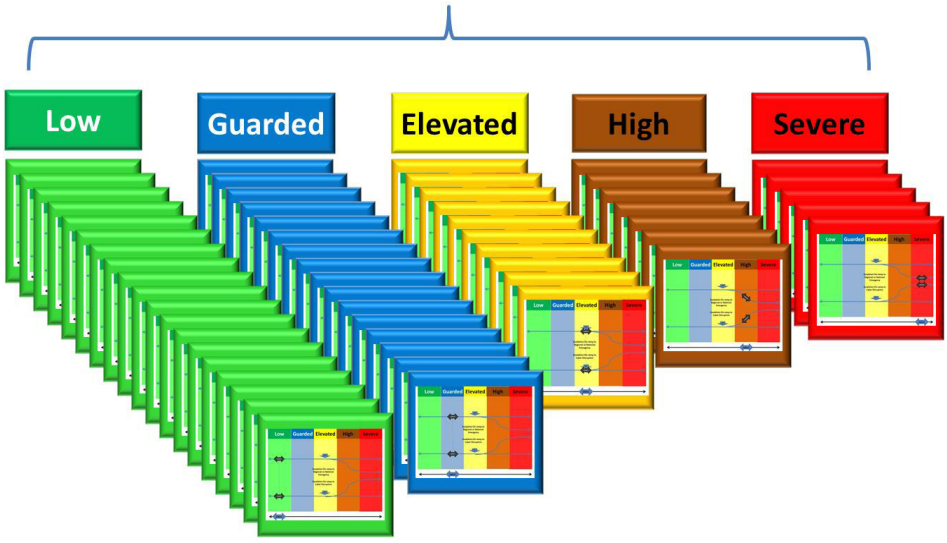
Collaboration between the cyber disruption response function and the emergency management function is essential. Given the integration of information technology with virtually any other discipline or line of business, these two functions will have to be engaged in almost any type of disruption or emergency. Further, it is conceivable that even during an emergency event that appears to be a natural disaster that cyber criminals or nation states who have an agenda to act against the United States will take advantage of such circumstances to launch a cyber attack in order to compromise this nation's ability to respond and recover from such an event. The parallel processes for state emergency management and the state information security officer can be represented as follows.



Interoperability between emergency management, cyber incident and cyber disruption management

The cyber event portfolio can be represented as follows. Any given cyber event will have an inherent lifecycle. It may stay at a single threat level or may move across the various threat levels during a particular event lifecycle. At any given point time, there will be many cyber events at various points in their lifecycles and occupying various threat levels.

Cyber and Emergency Event Portfolio



The subsequent sections of this report will describe on a proforma basis the various roles and interactions that must be established up front of any actual event. This cross-functional interaction is intended to guide individual states and territories in their own development of operating discipline regarding cyber disruption response planning. Therefore, this document should not simply be adopted. Rather, it should be reviewed in detail and modified to match the particular circumstances in each individual state or territory. This includes modifying as necessary the organization, roles, responsibilities and interactions describe herein.

The various threat levels that are described in this reference will present the threat level framework and how it may actually appear in the cyber event portfolio. For simplification, the event on the chart is categorized at the same threat level for emergency management and the CISO's office. In reality, a given event that touches both emergency management and cyber disruption could be a hybrid posing different threat levels for emergency management and cyber disruption. However, for purposes of this report, it is presumed that any cyber event is also posing the same level of threat to other aspects of state government. This seems realistic given the fact that all functions, infrastructure and emergency support functions depend on information technology, including networks, in order to operate.

☐ ***List of Stakeholders***

☐ Office of the Chief Information Officer ☐ Deputy Chief Information Officer (DCIO) ☐ Chief Technology Officer (CTO) ☐ Chief Information Security Officer (CISO) ☐ Enterprise Information Security Office (EISO) ☐ Enterprise Data Center (EDC) ☐ Continuity of Operations Plan Incident Command Team ☐ Agency Chief Information Officer (Agency CIO) ☐ Agency Cybersecurity Emergency Preparedness Liaison Officer (Agency Cybersecurity EPLO) ☐ Agency Information Security Officers (ISOs)	☐ State Government Service Providers ☐ State Government Business Partners ☐ State Emergency Management Agency (EMA) ☐ Cybersecurity Incident Response Team (CSIRT) ☐ Information Sharing and Analysis Center (ISAC) ☐ Governor's Office of Homeland Security (GOHS) ☐ State Police (SP) State Criminal Intelligence Center (CIC) ☐ National Guard Cyber Teams ☐ National Fusion Center Association Cyber Threat Sub Committee (NFCA-CTI) ☐ Multi-State Information Sharing and Analysis Center (MS-ISAC) ☐ DHS/Federal Emergency Management Agency (FEMA) ☐ U.S. Computer Emergency Readiness Team (US-CERT)

☐ ***Office of the State CIO (the CIO)***

When a cybersecurity event escalates to be classified as a cyber disruption the office of the state CIO (the CIO) will work with the Governor's Office, Office of the Budget, Chief Technology Officer (CTO), the Chief Information Security Officer (CISO) and the office of Emergency Management to identify the related issues and effects, and to assist in the remediation efforts. The CIO will also be responsible for communication with high level political officials and the media.

Note: All external communications about a cyber disruption need to be routed to the CIO or public information officer (PIO) for approval.

☐ ***Deputy CIOs***

A state CIO may have many deputies covering a variety of focus areas such as data, process, technology, cloud services, network, finance and communications. The team of deputies is responsible for establishing leadership and managerial oversight for state government IT resources. As with any cybersecurity event, during a cyber disruption this team will work with the CIO, Chief Technology Officer (CTO), and the Chief Information Security Officer (CISO) to identify the issues, related effects, and assist in the remediation efforts. This team of deputies will also be responsible for communications with the Agency Chief Information Officers and state government business partners.

☐ ***The Chief Technology Officer (CTO)***

The CTO in most cases reports to the state CIO and is responsible for the day-to-day operations of state IT infrastructure. During a cyber disruption, as with any cybersecurity event, the CTO will work with the CIO, Deputy CIOs, CISO, Agency Chief Information Officers (CIOs), relevant IT functions under the CIO, and emergency management to ensure that cybersecurity issues and effects are properly identified and remediated. The CTO will also be responsible for working with state emergency management to set up the senior management's emergency communications center and coordinated mitigation and recovery activities where man made or natural disasters intersect with a parallel cyber attack or a cyber disruption effect.

Note: A cyber attack may be launched in parallel to any number of disaster types in order to take advantage of a compromised circumstance. Any type of disaster typically handled by emergency management may have a cyber dimension or cyber disruption effect. A cyber disruption effect can include any effect that interrupts or diminishes information technology assets and their performance. For example, an avalanche may cause a network disconnect; ;a tornado may level a data center or destroy telecommunication for power distribution networks. Response to the natural disaster is hampered by the loss of network connections affecting communications, the web emergency operations center, and access to any number of routinely used emergency management applications.

☐ ***The State Chief Information Security Officer (CISO)***

The CISO reports to the CIO and is responsible for protecting the State's IT infrastructure from internal and external cybersecurity threats. This responsibility includes:

- ☐ Agency Liaison – The CISO is responsible for working with the Agency CIOs to address local and state-wide cybersecurity events.
- ☐ Multi State Information Sharing and Analysis (MS-ISAC) Point of Contact – The CISO is responsible for working with MS-ISAC to assist in state-wide, regional and national cybersecurity events and to communicate potential remediation procedures to agencies, counties, boroughs, and cities impacted by a cyber disruption.
- ☐ The state may have established a state-wide or regional Information Sharing and Analysis Center ([state or region]-ISAC). The state CISO would be the Chairman and responsible for ensuring that the state or regional ISAC communicates cybersecurity threat levels and provides local readiness and response within the state by providing a central resource for gathering information on cyber threats to critical infrastructure throughout the state and providing two-way sharing of information amongst local governments and other states encompassed by the event.
- ☐ Cybersecurity Incident Commander – The CISO will take the lead on any cybersecurity event that has state wide implications. When that event is both a cyber event and an emergency event, the CISO and the state Office of Emergency Management or Incident Commander will share this role.

- ☐ **State Emergency Operations Center (SEOC) Cybersecurity Emergency Preparedness Liaison Officer (EPLO) – The CISO will be the state CIO's representative at the SEOC during cyber event that reaches high or severe threat level.**
- ☐ State Cybersecurity Incident Response Team (state-CSIRT) – The CISO will be responsible for overseeing the state-CSIRT activities during a cybersecurity event.
- ☐ State Emergency Operations Plan (SEOP)/Emergency Support Function (SEOP/ESF) #2 – The CISO will ensure the Office for Information Security fulfills the responsibilities identified in the Cyber Incident Annex which is maintained by state Emergency Management Agency (EMA).
- ☐ **Federal Emergency Management Agency (FEMA) – The CISO in conjunction with EMA will work with FEMA to address cybersecurity incidents and disruptions that impact or are precipitated by national disaster recovery efforts.**
- ☐ U.S. Computer Emergency Readiness Team (US-CERT) – The CISO will ensure that the Office for Information Security works with US-CERT to gather and disseminate cybersecurity information and warnings to the state.
- ☐ Governor's Office of Homeland Security (GOHS) – The CISO will work with GOHS to assist them carry out their mission of enhancing the state's information and intelligence sharing capabilities with law enforcement on a state, local and national level, focusing on prevention, protection and mitigation.
- ☐ **State Criminal Intelligence Center (CIC) – The CISO will work with CIC to support their mission of assisting local, state, and federal law enforcement agencies with cyber terrorism and cyber criminal activity. This assistance may range from providing Subject Matter Experts (SMEs) to assist in the analysis of cyber threat information to providing cybersecurity training for the CIC analysts.**
- ☐ Service Providers – The CISO will work with the service providers listed in the state enterprise services portfolio to ensure they perform proper reporting and management of cybersecurity disruptions in order to secure and protect the state's critical IT business processes and assets from cyber threats.

Enterprise Information Security Office (EISO)

The EISO is responsible for the state's cybersecurity readiness, threat analysis, and remediation efforts. These responsibilities include:

- Proactive Cybersecurity Event Monitoring – The EISO will use MS-ISAC, Microsoft Bulletins, and other media outlets to proactively identify potential cybersecurity threats and take precautions before they impact they can cause potential to harm the state's IT infrastructure.
- State Security Threat Level – The EISO is responsible for setting and alerting the state regarding the current cybersecurity threat posture. For more information about this process, please reference the procedures section of this document.
- Cybersecurity Alerts – The EISO disseminates cyber threat warnings and information to state government agencies, private citizens, and business entities.
- Coordinating Recovery From Cybersecurity Attack/Event – During a cyber event the EISO will be responsible for coordinating the recovery of state network operations, telecommunications, and IT applications and databases.
- Remediation Efforts – The EISO coordinates remediation efforts with local government IT representatives through the (state-ISAC) and ISO to exchange policy and operational information necessary to respond to and recover from cybersecurity incidents.
- Agency Support – The EISO provide assistance to agencies in helping remediate issues caused by cybersecurity incidents.

- Cybersecurity Preparedness and Education – The EISO is responsible for preparing and educating state agencies, and employees as to the dangers of cybersecurity threats and how to reduce their risk exposure.
- Collaboration – The EISO facilitates interaction and collaboration among state agencies, state and local governments, business partners, private sector entities, and international organizations related to cybersecurity and cyber incidents.
- **Cybersecurity Advanced Analytics – The EISO will develop and exercise the capabilities for predictive analytics related to cybersecurity. Predictive capabilities include various analytics applied to a variety of data from any number of sectors but also include analysis of cyber incidents and disruptions to uncover broader based patterns of attack. Operating discipline will need to be developed that is highly predictive and interpretive in order to understand existing and emerging patterns affecting any line of business including: healthcare, power generation and distribution, water treatment and distribution, sewage treatment, agriculture, transportation, manufacturing, finance and banking.**
- Cybersecurity Forensic Analysis – The EISO supports the Department of Justice, Federal Bureau of Investigations, State Police and other law enforcement agencies in investigating and gathering of information related to cyber threats and attacks.
- **State-wide Cybersecurity Emergency Response – The EISO will work with the state EMA to coordinate remediation efforts from a cybersecurity event that jeopardizes the health and safety of the citizens of the state. Disseminates cyber threat warning information in conjunction with the state EMA.**
- State-Computer Security Incident Response Team (CSIRT) – During a cybersecurity event, the EISO will put together a state-CSIRT to provide event information and decision support, and coordinate response to cybersecurity issues. The state-CSIRT will provide technical and operational support to agencies, counties, cities, boroughs, and state government Business Partners impacted by a cybersecurity event.
- **SEOP/ESF 2 – The EISO will fulfill the responsibilities outlined in the Cyber Incident Annex which is maintained by the state EMA.**
- **FEMA – The EISO will work with the state EMA and FEMA to address cybersecurity disruptions that impact national disaster recovery efforts.**
- US-CERT – The EISO will work with US-CERT to gather and disseminates cybersecurity information and warnings to the state.
- **GOHS – The EISO work with GOHS to address issues that impact national security.**
- State CIC – The EISO will work with the state CIC to help review and disseminate cybersecurity threat information.
- Service Providers – The EISO will work with the various service providers to ensure they respond to and address cybersecurity incidents reported to them by the EISO and/or state agencies under the Governor's jurisdiction.

Enterprise Data Center (EDC)

The EDC is responsible for ensuring that the state's servers are patched properly and have the most current antivirus and intrusion detection software installed on them. During a cybersecurity event, the EDC will work with the EISO to resolve any issues that may be caused by a cyber disruption and may be required to initiate its Continuity Recovery Plan (CRP).

Continuity of Operations Plan Incident Command Team

In the event of activation or partial activation of the Continuity of Operations Plan (COOP), the COOP Incident Command Team has been identified and organized according to federal NIMS/ICS guidelines. To staff the COOP teams, the Governor's Office of Administration has identified key positions to provide management and technical expertise necessary to establish critical functions within 12 hours after the emergency event.

Agency Chief Information Officer (Agency CIO)

Each Agency CIO is responsible for the overall IT operations of his or her agency. During a cybersecurity event the CIO would act as the liaison between his or her Deputy CIO, CTO, CISO, EISO, Business Partners, and their staff.

Agency Cybersecurity Emergency Preparedness Liaison Officer (Agency Cybersecurity EPLO)

The Agency Cybersecurity EPLO is a person within the agencies who have been given the authority by the agency secretary to act as the agency's cybersecurity representative at the state EMA. During a cybersecurity event, this individual will:

- Represent the Agency – The Agency Cybersecurity EPLO will represent the agency from an IT perspective and they will have the authority to redirect IT resources (personnel, assets, etc.) to the remediation effort.
- Complete Emergency Purchase Orders – The Agency Cybersecurity EPLO will and be ability to complete emergency purchase orders to procure equipment, staff augmentations, backup facilities, etc.
- Enact the Agency COOP - The Agency Cybersecurity EPLO will have the authority to enact the agency's COOP.

Agency Information Security Officers (ISOs)

The ISOs are responsible for the day-to-day IT security administration of their agencies. During a cybersecurity event, the ISOs will report cybersecurity incidents to the CISO and the EISO. In addition to reporting incidents, Agency ISOs will:

- Agency Cybersecurity Level – ISOs will be responsible for monitoring their agency's internal cybersecurity level and reporting increases/decreases in their security levels to the EISO.
- Incident Reporting – Agency ISOs will be responsible for reporting cybersecurity incidents to their Agency CIOs and the EISO.
- Communication – ISOs will be responsible for communicating security related information to the Agency CIO, EISO, agency IT staff, business partners, users, etc.
- Remediation Efforts – ISOs will assist in agency remediation efforts.

State Government Service Providers

State government service providers support the EISO in its cybersecurity mission and will perform proper reporting and management of cybersecurity incidents in order to secure and protect the state's critical Information Technology (IT) business processes and assets from cyber-threats. As part of these responsibilities, service providers will provide:

- Technical and Operation Support – service providers will provide technical and operational support for EISO when a cybersecurity incident involves enterprise assets, multiple agencies, or outside entities such as business partners or citizens that are utilizing a service provider's controlled assets (appliances,

servers, firewalls, routers, etc), Incident handling processes are outlined in Section 6.4 and 6.5 for service providers and service provider/Level 3 respectively

- Points of Contact. These points of contact will be responsible for ensuring that cybersecurity incident reporting and handling is addressed within the timeframes identified by the state's incident response SLAs.
- Provide notification to the state-CSIRT within thirty (30) minutes of detection and incident reports need to be filed within four (4) hours of detection.
- Promptly investigate incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse, or access to information technology resources such as systems, files, and databases.
- Alert EISO of potential cybersecurity incidents discovered via their automated incident response, intrusion detection, and security event and incident management systems.
- Provide EISO with the names, work phone numbers, mobile phone numbers, home phone numbers, and work and home e-mail addresses for cybersecurity incident responders who can work with EISO to remediate cybersecurity incidents
- Cooperate with EISO cyber incident investigation and remediation efforts.
- Provide processes for ensuring that all service provider security operations and support (Provider SO&S) employees are aware of the state's cybersecurity policies and procedures.
- Ensure that the service provider security operations and support Service Desk personnel are aware of the internal/external cybersecurity incident response process and how to differentiate between network, telecom, and cybersecurity incidents.

State Government Business Partners

State Government Business Partners (SGBPs) are defined as companies and non-profit organizations that either provide support to the state IT infrastructure or who need access to it to provide services to citizens. During a cybersecurity incident, SGBPs would need to work with the DCIO, CTO, CISO, and the EISO to remediate any issues associated with the attack.

State Emergency Management Agency (State EMA)

The mission of EMA is to coordinate state agency response, including the Office of the State Fire Commissioner and Office of Homeland Security, to support county and local governments in the areas of civil defense, disaster mitigation and preparedness, planning, and response to and recovery from man-made or natural disasters. From a cybersecurity perspective EMA will:

- Work with the county emergency management agencies and communication centers to ensure that EMA's IT based resources are not impacted by a cyber-security event.
- Act as the incident commander for the counties and municipalities and collect, report, and remediate any cybersecurity threat that could impact disaster recovery efforts.
- Act as the state's backup cybersecurity operations center providing the office of the state CIO and agencies impacted by a cybersecurity event with meeting facilities and back-up communications (satellite feeds, wireless radios, etc.)

State Cybersecurity Incident Response Team ([state]CSIRT)

Enterprise incident response for computer security incidents within state government is a critical component to protecting state government resources. The goal of CSIRT is to assist and direct agencies in their handling

of security incidents. Agencies will be required to notify CSIRT of security incidents in order to ensure incidents are handled properly and security metrics can be collected. CSIRT also provides a means for notifying agencies of threats, vulnerabilities and enterprise incidents.

CSIRT offers many services to an organization, such as computer forensics, alerts & advisories, incident handling, vulnerability assessments, risk analysis, awareness training, product evaluation and more.

State Information Sharing and Analysis Center ([state]-ISAC)

The state ISAC is responsible for addressing cybersecurity readiness and critical infrastructure coordination. The state ISAC is led by the CISO who is responsible for leading the state's efforts regarding cyber readiness and resilience. The ISAC provides a common mechanism for raising the level of cybersecurity readiness and response within state government by providing a central resource for gathering information on cyber threats to critical infrastructure throughout the state and providing two-way sharing of information between and among local governments.

Governor's Office of Homeland Security (GOHS)

GOHS manages overall protection framework and oversees the implementation and continual evaluation of the state's Critical Infrastructure Protection Program. This program is comprised of six objectives which include: identifying assets; assessing risks; prioritizing disaster recovery; implementing protective programs; and measuring effectiveness.

During a cybersecurity event, GOHS will monitor the situation to make sure that event isn't tied to a terrorist attack. If this occurs, GOHS will act as a liaison between the Federal Department of Homeland Security (DHS) to help coordinate federal resources and assist in the recovery process.

State Police (SP) Criminal Intelligence Center (CIC)

The State Police, Bureau of Criminal Investigation provides law enforcement agencies throughout the state with one central point of contact for their information needs. Through the CIC, trained analysts provide state police members and federal, state, and municipal law enforcement officers with access to intelligence information, investigative data, and public source information 24 hours a day, seven days per week. Analysts also provide investigative support by analyzing complex information and collating it into intelligence summaries, organization charts, link analysis, time event analysis, and other manageable, professional products.

During a cyber event, the CIC will work with the EISO to help identify, document, and collect forensic evidence for potential prosecution. In addition to this, the CIC will help coordinate investigations that involve the Department of Homeland Security and the Federal Bureau of Investigation's cyber law enforcement agencies to prosecute cyber criminals that may reside in other states and nation states.

National Guard Cyber Teams

The National Guard (NG) is comprised of both the Air National Guard (ANG) and Army National Guard (ARNG). In peacetime, the governor serves as commander in chief of the NG, exercising control through the adjutant general.

In the event of natural disaster or civil emergency, the governor can order the NG personnel and equipment into service to assist state and local authorities. As part of this mission, the NG has created teams of part-time soldiers and airmen who work as cybersecurity experts in the private and public sectors.

During a large scale cyber event, the Governor will activate NG cyber teams to help assist state and local governments with combating and restoring critical infrastructure (dams, power plants, mass transit, etc.) and services that have been damaged of lost from cyber attacks. In addition to recovery, the NG will work with Governor's Office, EMA and the SP to setup alternate forms of telecommunications (satellite, cellular, shortwave, etc.) and assist with physical security at critical infrastructure and alternate recovery sites.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

The MS-ISAC is a collaborative organization with participation from all 50 States, the District of Columbia, local governments and U.S. Territories. The mission of the MS-ISAC is to provide a common mechanism for raising the level of cybersecurity readiness and response in each state and with local governments.

DHS/Federal Emergency Management Agency (FEMA)

FEMA provides communications and IT support to Joint Field Office operations, and coordinates the restoration of Public Safety Communications systems and first-responder networks. During a cybersecurity event, FEMA works with the National Communications System (NCS) to provide communications support to the impacted area and ensures that and assists in the remediation efforts.

U.S. Computer Emergency Readiness Team (US-CERT)

US-CERT is a 24/7 operations center with connectivity to all major federal cyber operations centers and private sector Internet service providers, information sharing mechanisms, and vendors. During a cyber event, US-CERT acts as a focal point to collect and disseminate cybersecurity information received from public and private sector sources. In addition to disseminating information, USCERT provides technical and operational support to the Interagency Incident Management Group and interacts with private and public sectors on a continuous basis throughout the extent of the incident.

Fusion Centers (NFCA-CTI)

A fusion center addresses both strategic and technical cyber analysis and has the capability to provide strategic intelligence that focuses on the integration of international, national, and domain-specific intelligence with cross-programmatic issues pertinent to national security and public safety, as well as specialized case support and highly technical intelligence. The inclusion of tactical analysis allows a fusion center to support case development with resources and expertise that are not widely available.

FBI Cyber Shield Alliance www.iacpcybercenter.org/resource-center/fbi-cyber-shield-alliance/

Cyber Shield Alliance (CSA) is an FBI cyber security partnership initiative developed by law enforcement for law enforcement to proactively defend and counter cyber threats against law enforcement networks and critical technologies. CSA encourages law enforcement participation as a force multiplier in defending our national security, while equipping agencies with the training and tools to optimize and defend their own law enforcement networks. For CSA's partners in state and local law enforcement, Cyber Shield Alliance is accessible via the Law Enforcement Enterprise Portal (LEEP) at www.cjis.gov as well as the Regional Information Sharing Systems (RISS) at www.riss.net .

These capabilities make the fusion center an essential member of any Cyber Disruption Team.

Cybersecurity Alert Escalation/De-escalation Procedures

The state's cybersecurity threat level is broken into various categories that describe the threat level. Some state have defined four levels. Some have defined five levels. States use different names and different colors for these categories. This document borrows from the Commonwealth of Pennsylvania and uses five categories. Each of these levels can be impacted by internal and external cybersecurity events. Each category contains the following sections:

- Level Definition – This section contains a brief description of what each security level means.
- Escalation/De-escalation Criterion – Each section will provide a description of what variables are needed to be in place for the alert level to change.
- Potential Impact – This section explains how the level impacts the state's agencies, business partners, local governments, and citizens.
- Communication Procedures – This section describe how the EISO will communicate to the individuals and organizations impacted by the cybersecurity event.
- Responsibilities – This section describes what each group within the state needs to do to ensure that governmental IT operations are functioning during each level.

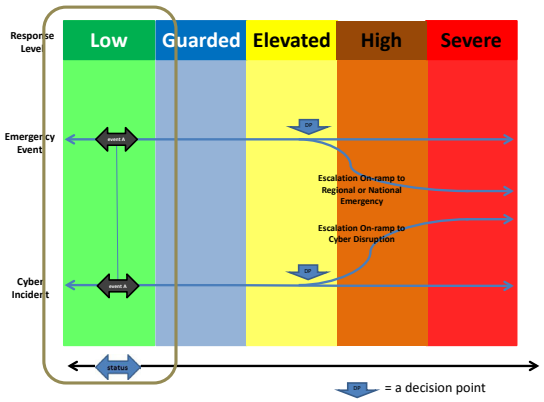
Note: The threat levels in this document are based on the risk an event poses and the impact it has on the state government enterprise. There may be times when an incident may require EISO to skip levels to address the threat and then return to the originating level after the threat has been mitigated.

Green or Low

Green is the lowest level in the cybersecurity threat matrix. The following will explain what this level means and the impact it has on state agencies, business partners, local governments, and citizens.

- Level Definition – Green indicates that insignificant or no malicious activity has been identified. Examples include but not limited to:
  - Credible warnings of increased probes or scans.
  - Infected by known low risk malware.
  - Other like incidents.
  - Normal activity with low level of impact.

  Actions:
  - Continue routine preventative measures including application of vendor security patches and updates to anti-virus software signature files on a regular basis.
  - Continue routine security monitoring.
  - Determine baseline of activity for state – that is it is important to know what "normal" looks like – and then continually be on alert for any changes to that baseline.
  - Ensure all personnel receive proper training on Cybersecurity policies and security best practices.



- Escalation Criterion – This level is considered to be the IT baseline level where the infrastructure is operating normally and there are no major known cyber threats on the horizon.
- De-Escalation Criterion – In order to return to this level the conditions that caused the change must be remediated.

- Potential Impact – The threat level is low which means that there should be no cyber related issues impacting state IT resources.

  Note: Any type of IT disruption or anomalies should be reported to the EISO so it can look into the matter to determine if the disturbance is cybersecurity related or if it is caused by planned IT related functions like PATCH management or firewall reconfiguration.
- Communication Procedures – Besides the day-to-day operational communications, there are no special communication procedures required while the state is at this level.
- Responsibilities – When the state is at this level the following groups will be active and will carry out their assigned duties:
  - EISO – The EISO will be responsible for the following functions:
    - **Threat Monitoring - The EISO and will monitor the national and international cybersecurity threat levels and cybersecurity informational resources to identify and report on potential threats that could impact the state. The fusion will be a key partner in conducting threat monitoring.**
      - Fusion Center provides advanced intelligence on current and emerging threats. The fusion center will notify stakeholders based on the nature and analysis of the threat.
    - Cybersecurity News and Information Sharing – The EISO will use the cybersecurity portal and the state ISAC to post information on emerging cybersecurity threats and ways to combat them.
    - Email Notifications – The EISO will use the state ISAC portal to send members cybersecurity news and updates.
    - Log Validation – The EISO will review the security logs to determine if there are any suspicious network activity (bot, spyware, malware, virus, etc.).
    - Validation Assessments – The EISO will use vulnerability and penetration tools to ensure that agencies have the most recent patches and antivirus agents, engines, and definitions.
    - White Hat Hacking – The EISO will proactively try to hack state IT resources to discover potential flaws that could lead to: data breaches, hijacking, theft of services, etc.
    - Anomaly Investigation – The EISO will investigate reports of network issues (slowdowns, disconnections, disrupted services, etc.) to determine if the cause of the problem is due to technical issues or a cyber attack.
    - GOHS and CIC – The EISO will support GOHS and the state's CIC with their Cybersecurity missions.
  - State Government Service Providers security operations and support (Provider SO&S) – Will work with the EISO to identify and address potential cybersecurity incidents discovered by their security monitoring tools or reported to them by agencies, users, etc.
  - The state's EISO is responsible for installing and monitoring server-based security agents on servers located in the Enterprise Data Center (EDC). The state EISO will also be responsible for:
    - 24/7 Hotline – SOS will provide 24/7 security support for EDC and state agencies.
    - Managing Enterprise Firewalls – SOS will monitor the enterprise firewall logs to ensure they are in place and working properly and assist the EISO with firewall blocks against IPs that pose a threat to the network.
    - Reporting Incidents – SOS will report all cybersecurity incidents to the EISO so that it can investigate them.

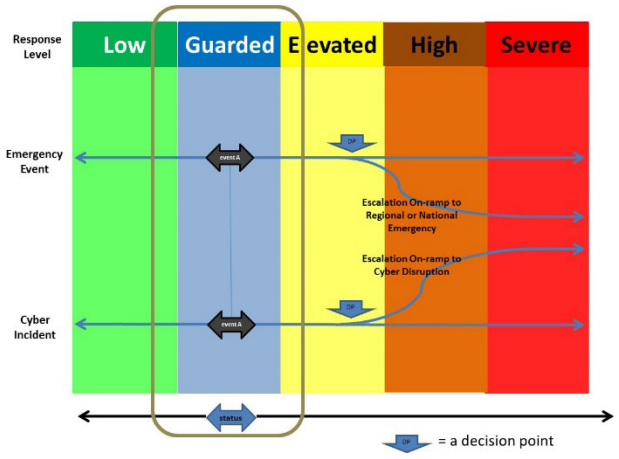
- Enterprise Data Center (EDC) is responsible for managing the enterprise servers in the server farm and the security agents that are installed on them. During a code green alert, the EDC will be responsible for:
  - Patch Management – EDC will ensure that all of the enterprise severs have the most current operating system patches installed on them and that the patch is installed correctly.
  - Antivirus Agents/Antivirus Signatures – EDC will ensure that all of the enterprise severs have the most current antivirus security agents and that they are updated with the most current signatures.
  - Internet Information Services (IIS) – EDC will ensure that the IIS is in place and working properly. In addition to this, SOS will work with the EDC to monitor the ISS logs for any suspicious activity and report it to the EISO so that it can investigate it.
  - Microsoft Operations Manager (MOM) – EDC will monitor the MOM logs and alerts for server availability and out of the ordinary Operating system level events and report it to the EISO.
  - Firewall Management – the SOS and the EDC will monitor the EDC firewall logs to ensure they are in place and working properly. In addition to this, EDC will review and execute requested firewall changes.
- Agency ISOs – Agency ISOs are responsible for working with the EISO to help identify and report on cybersecurity events that could impact their agencies' and the state's IT infrastructure. In addition to identifying potential cybersecurity events, the ISOs is responsible for:
  - Reporting Cybersecurity Incidents – ISOs are responsible for reporting agency specific cybersecurity incident(s) to the EISO. Incidents can range from data breaches to unexplained network issues/ traffic.
  - Agency Cybersecurity Alert Level – The ISOs are responsible for monitoring their agencies' cybersecurity readiness and their internal threat level. This level should be increased when they have a confirmed cybersecurity incident or during times that their respective agency could be at greater risks of attack (tax season, elections, etc.).
- GOHS – GOHS will continue to support the cyber mission by meeting with the federal, state, and local government officials and state based business owners to determine their cybersecurity readiness and communicating this information to the EISO and CIC.
- CIC – Will work with the EISO, GOHS, and the FBI to identify potential threats that could impact the state and its business partners.

Blue or Guarded
Blues the first step in cybersecurity threat level. The following will explain what this level means and the impact it has on state government.

- Level Definition – At this level, malicious activity has been identified with minor impact. Examples include but not limited to:
- Change in normal activity with minor level impact.
- A vulnerability is being exploited and there has been minor impact.
- Infected by malware with the potential to spread quickly.
- Compromise of non-critical system(s) that did not result in loss of sensitive data.
- A distributed denial of service attack with minor impact.

Actions:

- Continue recommended actions from previous level.
- Identify vulnerable systems and implement appropriate counter-measures.
- Identify malware on system and remediate accordingly.
- Data exposure with minor impact.
- When available, test and implement patches, install anti-virus updates, etc. in next regular cycle.
- Contact MS-ISAC for any additional guidance.



- Escalation – In order to raise the state or agency threat level to blue, the following conditions must be in place:
  - Risk Level – The threat is limited to one agency, application, or website; and/or the risk of the threat is so low and it can be easily remediated without having a long-term impact to state, business partners, local governments, and citizens.
  - Impact to IT Services – At level blue, the following conditions are in place:
    - Impact – There is no threat to mission critical applications or resources; and the issue has been properly identified and it can easily be remediated without risk of a data breach or theft of services.
    - Time – The issue can be remediated within normal business hours.
    - Remediation Effort – The threat can be easily remediated by the state agencies installing software patches, updating the antivirus files, or denying network access to specific IPs or IP ranges.
  - Special Events/Circumstances – There is a special event or circumstance that might make hackers/crackers interested in trying to disrupt the agency's IT services it or cause political embarrassment (Website Defacements, Application Hacking, etc.)
- Agency Impact – IT staff will have to take some proactive measures (patches, updating anti-virus files, etc.) to address the potential issue but impact to IT services should be minimal since the threat has been identified there are ways to quickly address it without impacting IT services.
- Communication Procedures – A blue or guarded situation means that all of IT resources are still operational. This means that the following communication mediums will be utilized:
  - Cybersecurity Portal – The EISO will use the cybersecurity portal to:
    - Post Information – The EISO will use its portal to post the cybersecurity current threat level and IT security information such as alerts, MS and Linux Bulletins, etc.

    - Incident Reports – ISOs and IT staff will use the portal to submit cyber related security information such as equipment theft (PCs, Laptops, Digital Certificates, etc.) data breaches, and theft of services.
  - E-mail – E-mail will be used to communicate alerts, status reports, updates, and ancillary information.
  - Telecommunications – Land lines and cell phones will be used for clarification purposes and to address questions about remediation efforts.
- De-Escalation Criterion – In order to return to green, the issue must be completely resolved and the agencies confirm that the IT resources are working normally; and/or the special event has passed and there is no longer a need to take additional security measures.
- Responsibilities – When the state is at this level the following groups will be active and will carry out their assigned duties:
  - Fusion Center - provides advanced intelligence on current and emerging threats. As a threat increases in severity the fusion center will direct more resources toward monitoring the nature and behavior of the threat in terms of probability and magnitude of effects. The fusion center will notify stakeholders of its current assessment of the threat.
  - State CIO – The CISO will notify the state CIO when an incident causes the state to escalate the cybersecurity threat level from green to blue. The state CIO will then work with the Deputy CIOs and agency CIOs to make sure they comply with the remediation recommendations provided to them by the CISO and EISO.
  - Deputy CIOs – The DCIOs will ensure that all of the agencies are aware of the change in the state's alert level and ensure that the agencies within their auspices increase their security posture and/or take the corrective actions recommended by the CISO and EISO.
  - CTO – The CTO will be responsible for communicating with the state CIO, Deputy CIO, and the Agency CIOs. In addition to this, the CTO will ensure that all of the executive branch agencies within his or her auspices assist with the remediation efforts.
  - CISO – The CISO will work with the CIO and CTO to assist with communications and the remediation efforts. The CISO will also coordinate any communications that occur between state agencies, MSISAC, and the state ISAC.
  - EISO – The EISO is responsible for notifying agencies when the alert level changes from green to blue. In addition to this, the EISO will:
    - Incident Reports – The EISO will investigate incidents reported to them by the Agency ISOs, Agency IT staff, or state employees.
    - Raising the Alert Level – The EISO will raise the alert level to blue or Guarded and notify the CIO's Executive Management Team, Security Operations Section, Enterprise Data Center, Agency CIOs, and Agency ISOs of the change and the reason for it.
    - Updating the EISO Cybersecurity Portal – The EISO will change the level on the cybersecurity portal. The EISO in collaboration with the Public Information Officer will provide Local agencies and citizens with information about the threat and ways to avert it.
    - ISAC – EISO will work with the CISO to create advisories that go out the ISAC members.
    - MS-ISAC – EISO may need to contact MS-ISAC to get more information about potential attacks or to request clarification on remediation efforts.
    - Remediation Efforts – The EISO will assist agencies with remediating the issues that are impacting their IT resources.
    - De-Escalation Process – The EISO will ensure that the issues that caused the alert level to be raised have been addressed before lowering the level back to green.

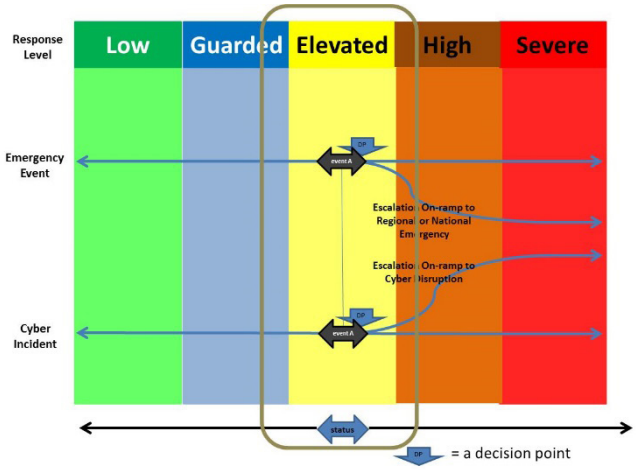
- GOHS and CIC – The EISO will send Governor's Office of Homeland Security (GOHS) and the state Criminal Intelligence Center (CIC) an email notification appraising them of the situation and to let them know if any assistance is needed.

- State government service providers Security Operations Center(SOC) – Will work with the EISO to identify and address potential cybersecurity incidents discovered by their security monitoring tools or reported to them by agencies, users, citizens, etc.
- State EISO will identify and address potential cybersecurity incidents discovered by state agencies and functions or state government service providers. In addition to this, the EISO will:
  - Incident Response – investigate any cybersecurity related incidents reported to their 24/7 Hotline.
  - Enterprise Firewall Management –identify and block IPs that attacks are originating from.
  - Remediation Effort –designate team members to work with the EISO to remediate the issue(s).
- State EDC – The state EDC will work with the EISO to identify the appropriate actions necessary to remediate the threat. In addition to this, the EDC will:
  - Security Monitoring Tools – EDC will report any anomalies to the EISO.
  - PATCH Management – EDC will work with the EISO to identify the proper application patches and ensure they are installed on the servers that would be impacted by the threat.
  - Antivirus – EDC will ensure that all of the servers have the most current antivirus agents and files installed and that they are working correctly.
- State-CSIRT – CSIRT team members will be put on alert and they may be called upon to assist agencies in their remediation efforts.
- Agency CIO – The Agency CIO will work with their Deputy CIO and their Communities of Practice to address any concerns or issues; and to coordinate remediation efforts that may require assistance from EISO or other agencies within their Communities of Practice.
- ISOs – ISOs will work with their Agency CIO to help coordinate remediation efforts. In addition to this, ISOs will be responsible for:
  - Agency Alert Level – ISOs will be monitoring the incident and adjusting their Agency Alert level to properly match their readiness and remediation efforts.
  - Incident Reporting – ISOs are responsible reporting any incident that may come about during the remediation efforts or that may have caused the agency to raise its alert level.
  - Communication – ISOs will work with the Agency CIO, EISO, the state EDC, Agency IT Staff, and their customers to identify and communicate information about the incident and remediation efforts.
- Agency IT Staff – The Agency IT Staff will work with the ISOs, EISO, the state EDC to identify and remediate issues that are impacting their IT resources.
- State Government Service Providers (SPs) and other Business Partners (BPs) – BPs should reach out to their respective agency representatives to make sure they are aware the change in security (or threat) level and to take additional proactive measures to secure their IT infrastructure.
- GOHS – GOHS will contact will be alerted to the situation and monitor federal DHS informational resources to see if the threat is potentially linked to cyber terrorist activities and provide the EISO and CIC with information that could help identify and mitigate the threat.
- State CIC – Will work with the EISO, GOHS, and the FBI to identify potential threats that could impact the state and its business partners. The CIC will be called upon to assist the EISO with the event if it is determined to be criminal in nature.

Yellow or Elevated

Yellow or elevated is the third threat level in cybersecurity threat matrix. The following will explain what this level means and the impact it has on the state.

- Level Definition – At this level, malicious activity has been identified with a moderate level of damage or disruption. Examples include but not limited to:
  - An exploit for a vulnerability that has a moderate level of damage.
  - Compromise of secure or critical system(s)
  - Compromise of systems containing sensitive information or non-sensitive information.
  - More than one entity (agency) affected in your network with moderate level of impact.
  - Infected by malware that is spreading quickly throughout the Internet with moderate impact.
  - A distributed denial of service attack with moderate impact.



  Actions:
  - Continue recommended actions from previous levels.
  - Identify vulnerable systems.
  - Increase monitoring of critical systems.
  - Data exposure with moderate impact
  - Contact MS-ISAC SOC for additional guidance.
  - If this event is an Advanced Persistent Threat (APT) activity, steps other than the ones listed must be taken. Please contact the MS-ISAC SOC for guidance.
  - Immediately implement appropriate counter-measures to protect vulnerable critical systems.
  - When available, test and implement patches, install anti-virus updates, etc. as soon as possible
- Escalation – In order to raise the state or agency threat level to yellow, the following conditions must be in place:
  - Risk Level – The threat involves two or more agencies, critical applications, or websites; and/or the risk of the threat is has been determined to have a significant impact to state IT operations.
  - Impact to IT Services – At level yellow, the following conditions are in place:
    - Impact
      - An exploit for a critical vulnerability exists and it has the potential to cause significant damage if exploited.
      - There are multiple web defacements.
      - A critical vulnerability is being exploited and there has been moderate impact.
      - Attackers have gained administrative privileges on compromised systems.
      - Critical applications or resources have been impacted.
      - Compromise of secure or critical system(s) containing sensitive information.
      - Compromise of critical system(s) containing non-sensitive information if appropriate.
      - IT Services may be interrupted by denial of service attacks.

  - Time – The issue can be remediated within one to three business days and may require that the critical application or services be taken offline until the issue can be remediated.
  - **The State Continuity of Operations Plan/ Continuance of Government (COOP/COG) may have to be initiated to address the damages from the cyber attack.**
  - Remediation Effort – The threat can be remediated by state agencies installing software patches, updating the antivirus files, or denying network access to specific IPs or IP ranges.
  - Agency Impact
    - Agency IT staff will work with the EISO to install software patches, update antivirus files, or deny network access to specific IPs or IP ranges.
    - **The Agency CIOs will work with the DCIO, Office of General Counsel and Press Secretary to address any political or legal ramifications that may arise from the incident.**
    - **Cybersecurity EPLO will work with EMA to address any communication or facility needs the agency may need to address the incident.**

- **Communication Procedures – Yellow or elevated situation means that some of the state's IT critical resources have been impacted by a cybersecurity event or that multiple agencies have had significant security breaches. A this level, the following communication mediums will be utilized:**
  - EMA – EMA will be notified via email, telephone, or cell phone and they will start making preparations to enact their internal cybersecurity emergency response plan.
  - MS-ISAC – EISO will notify MS- ISAC via a secure portal, e-mail, or telephone. The EISO may also request assistance from MS-ISAC with remediating the issue.
  - State-ISAC – EISO will provide ISAC members with updates or remediation information.
  - Cybersecurity Portal – The EISO will continue to use cybersecurity portal to provide agencies and the citizenry with pertinent information.
  - E-mail – E-mail will be used to communicate alerts, status reports, updates, and ancillary information.
  - Telecommunications – Land lines and cell phones will be used for clarification purposes and to address questions about remediation efforts.
- De-Escalation Criterion – In order to return to blue or guarded, the incident must meet the escalation criterion identified within that section; and/or the special event has passed and there is no longer a need to take additional security measures.
- **Responsibilities – When the state is at this level the following groups will be active and will carry out their assigned duties:**
  - Office of the state CIO – At yellow, the state CIO will contact the Secretary of Administration to brief him or her on the situation. The state CIO will also contact the Deputy CIO and Agency CIOs to talk about potential contingency plans.
  - Fusion Center - provides advanced intelligence on current and emerging threats. As a threat increases in severity the fusion center will direct more resources toward monitoring the nature and behavior of the threat in terms of probability and magnitude of effects. The fusion center will notify stakeholders of its current assessment of the threat.
  - Agency CIOs – The Agency CIOs will ensure that all of the agencies within their Communities of Practice are aware of the change in the state's alert level and assist the agencies impacted by the incident by relocating IT resources to address the issues identified by the CISO and EISO.
  - CTO – The CTO will be responsible for working with the state CIO, Deputy CIO, and the Agency CIOs to provide them with technical assistance in remediating the issues caused by incident(s).

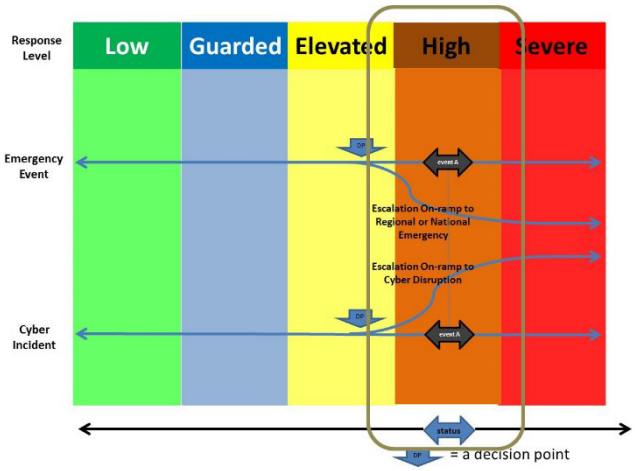
- CISO – The CISO in conjunction with EISO will work with the CTO and assist with communications that identify the issues and the remediation efforts. **The CISO will also contact EMA's State Emergency Operations Center (SEOC) to brief them on the situation and to give them time to start making preparations for setting up an emergency operations center.**
- EISO – EISO is responsible for:
  - Incident Reports – The EISO will continue to document and investigate incidents reported to them by the ISOs, Agency IT staff, or state employees.
  - Raising the Alert Level – The EISO will raise the alert level to yellow or elevated and notify the State CIO Executive Management Team, EDC, Agency CIOs, and ISOs of the change and the reason for it.
  - Updating the EISO Cybersecurity Portal – The EISO will change the level on the cybersecurity portal and collaborate with the Public Information Officer to provide Local agencies and citizens with information about the threat and ways to avert it.
  - Notifying MS-ISAC – The EISO will notify the Multi-State ISAC via secure portal e-mail or telephone.
  - Increase monitoring of critical systems - The EISO will monitor the state's critical systems to ensure that the cybersecurity event is not affecting their operational status.
  - Remediation Efforts – The EISO will immediately implement appropriate counter-measures to protect vulnerable critical systems. EISO will also continue recommended actions from previous levels and assist agencies with remediating the issues that are impacting their IT resources.
  - De-Escalation Process – The EISO will ensure that the issues that caused the alert level to be raised have been addressed before lowering the level back to blue.
  - GOHS and CIC – If this is a new event, the EISO will send GOHS and CIC an email notification appraising them of the situation and to let them know if any assistance is needed. If it is an escalated event, the EISO will let them know what happened to change the alert level.
- State Government Service Provider SOCs – Will work with the EISO to identify and address potential cybersecurity incidents discovered by their security monitoring tools or reported to them by agencies, users, citizens, etc. Service Providers may also need to block IPs, blackhole DNS, etc.
- The EISO will identify and block IPs that attacks are originating from and work with our Business Partners to identify and remediate the issue(s).
- EDC – EDC will work with the EISO to identify the appropriate actions necessary to remediate the threat. In addition to this, the office of the state CIO will address the following:
  - Security Monitoring Tools – EDC will report any anomalies to the EISO.
  - PATCH Management – EDC will work with the EISO to identify the proper application patches and ensure they are installed on the servers that would be impacted by the threat.
  - Antivirus – EDC will ensure that all of the servers have the most current antivirus agents and files installed and that they are working correctly.
- State-CSIRT – State-CSIRT team members will be put on alert and they may be called upon to assist agencies in their remediation efforts.
- Agency CIO – The Agency CIO will work with their Deputy CIO and their Communities of Practice to address any concerns or issues; and to coordinate remediation efforts that may require assistance from the StateCSIRT, EISO, or other agencies within their Communities of Practice. **Depending upon the event and its impact on the agency, the Agency CIO may need to activate it disaster recovery plan.**

- ISOs – ISOs will work with their Agency CIO to help coordinate remediation efforts. In addition to this, ISOs will be responsible for:
  - Agency Alert Level – ISOs will be monitoring the incident and adjusting their Agency Alert level to properly match their readiness and remediation efforts.
  - Incident Reporting – ISOs are responsible for reporting any incident that may come about during the remediation efforts or that may have caused the agency to raise its alert level.
  - Communication – ISOs will work with the Agency CIO, EISO, state CIO SOS, EDC, Agency IT Staff, and their customers to identify and communicate information about the incident and remediation efforts.
- Agency IT Staff – The Agency IT Staff will work with the ISOs, EISO, EDC to identify and remediate issues that are impacting their IT resources.
- Service Providers (SPs) and Business Partners (BPs) – SPs and BPs should reach out to their respective agency representatives to see if they need to assist in the remediation effort.
- **GOHS – GOHS will reach out to their federal and local contact to apprise them of the situation and to determine if the event is isolated to the one particular state government or part of a larger attack being conducted by a nation state or cyber terroristic group.**
- **State CIC – State CIC will work with law enforcement and DHS to determine if the event is criminal related. In addition to the criminal investigation, the state CIC may be called upon to help the with the remediation effort.**

Orange or High

At this level, there are confirmed cyber attacks that are disrupting federal, state, and local government communications; and/or there are unknown exploits that have compromised the state's IT resources and are using them to propagate the attack or to spread misinformation.

- Level Definition – At this level, malicious activity has been identified with a major level of damage or disruption. Examples include but not limited to:
  - Malicious activity impacting core infrastructure.
  - A vulnerability is being exploited and there has been major impact.
  - Data exposed with major impact.
  - Multiple system compromises or compromises of critical infrastructure.
  - Attackers have gained administrative privileges on compromised systems.
  - Multiple damaging or disruptive malware infections.
  - Mission critical application failures but no imminent impact on the health, safety or economic security of the State.
  - A distributed denial of service attack with major impact.



Actions:

- Continue recommended actions from previous levels.
- Contact MS-ISAC SOC for additional guidance.
- If this event is APT activity, steps other than the ones listed must be taken. Please contact the MS-ISAC SOC for guidance.

- Closely monitor security mechanisms including firewalls, web log files, anti-virus gateways, system log files, etc. for unusual activity.
- Consider limiting or shutting down less critical connections to external networks such as the Internet.
- Consider isolating less mission critical internal networks to contain or limit the potential of an incident.
- Consider use of alternative methods of communication such as phone, fax or state radio network in lieu of e-mail and other forms of electronic communication.
- When available, test and implement patches, anti-virus updates, etc. immediately.

- Escalation – In order to raise the state or agency threat level to orange, the following conditions must be in place:
  - Risk Level – The threat has the potential to impact multiple agencies and/or could require the state to shut down the IT infrastructure for five to ten business days to restore normal business operations.
  - Impact to IT Services – At orange, the following conditions are in place:
    - Impact
      - A critical vulnerability is being exploited and there has been significant impact.
      - Telecommunications may be interrupted causing agencies to use alternate forms of communication (cell phones, radios, messengers, etc.).
      - E-mail communications may be disrupted making it necessary for agencies impacted by the event to use alternate forms of communication.
      - State CIO Executive Staff may have to be relocated to the state EMA for command and control purposes.
      - Agency IT Operations may have to be relocated to the state EMA for command and control purposes.
      - COOP may have to be implemented to restore IT operations.
      - Power may become unreliable/unavailable for extended periods of time.
      - Multiple damaging or disruptive virus attacks; and/or, multiple denial of service attacks against critical infrastructure services.
    - Time – The issue can be remediated within five – ten business days and may require that the critical applications or services be taken offline until the issue can be remediated.
    - The state Continuity of Operations Plan/ Continuance of Government (COOP/COG) will need to be initiated to address the damages from the cyber attack.
    - Remediation Effort – The threat can only be remediated by restoring the applications and systems to an operational state by rebuilding equipment, restoring critical systems, or applications to a previous date before the attacks occurred.
    - Agency Impact
      - Agency IT staff will work with the office of the state CIO to restore their equipment, systems, and applications to an operational state.
      - The Agency CIO will work with the DCIO, Office of General Counsel and Press Secretary to address any political or legal ramifications that may arise from the incident.
      - Cybersecurity EPLO may need to relocate to the state EMA and work with the state CIO and their agency IT staff to restore IT Operations.

- Communication Procedures – At orange the state's IT critical resources have been severely impacted by a cybersecurity event that has caused IT service offline for an extended period of time. This event may be impacting telecommunications and may cause incident responders to use alternate forms of communications (radios, satellite phones, messengers, etc.).
  - State EMA – the state EMA will be notified via email, telephone, cell phone or messenger and they will start making preparations to enact their internal cybersecurity emergency response plan. In addition to this, the EMA will:
    - Provide executive meeting and conference rooms for the CIO, DCIO, CTO, Agency CIOs, and CISO to assist with the recovery process.
    - Provide operational meeting and conference rooms for EPLOs and Agency IT staff assisting with restoring telecommunications.
    - Establish temporary communications (radio, messengers, etc.) for recovery personnel.
  - MS-ISAC – EISO will contact MS-ISAC via email or telephone and if necessary request assistance with remediating the issue.
  - Fusion Center - provides advanced intelligence on current and emerging threats. As a threat increases in severity the fusion center will direct more resources toward monitoring the nature and behavior of the threat in terms of probability and magnitude of effects. The fusion center will notify stakeholders of its current assessment of the threat.
  - State-ISAC – EISO use the EMA's will provide stateISAC members with an update or the share remediation data.
  - Cybersecurity Portal – The EISO will continue to use cybersecurity portal to provide agencies and the citizenry with pertinent information.
  - E-mail – E-mail will be used to communicate alerts, status reports, updates, and ancillary information.
  - Telecommunications – Telecommunications may become unreliable making it necessary for first responders to use alternate forms of communication.
  - Radios – At orange, the EMA will issue radios to first responders who will be assisting in the recovery process.
  - Messengers – Depending on the nature of the event, the state may have to use messengers to communicate information between incident responders and the state CIO Command and Control Center.
- De-Escalation Criterion – In order to return to yellow, the incident must meet the escalation criterion identified within that section; and/or the special event has passed and there is no longer a need to take additional security measures.
- Responsibilities – When state government is at this level the following groups will be active and will carry out their assigned duties:
  - The office of the state CIO – At orange, the state CIO will contact the Office of the Governor to let him or her know about the severity of the situation. In addition to this, the state CIO will:
    - Determine if COOP should be activated.
    - Determine if the office of the state CIO should relocate its IT administration to the state EMA for command, control, and communication purposes.
    - Contact the Deputy CIO to talk about the contingency plans.
    - Assist the Governor, the Secretary of Administration and other cabinet members with:
      - Crafting sensitive communications to politicians, media, etc.
      - Contacting the Office of the Budget get emergency funding to replace equipment and resources damaged or destroyed by the event.

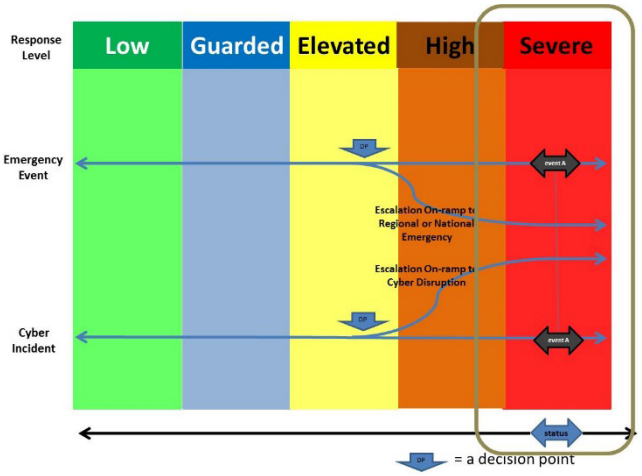
- DCIO – The DCIO will work with the CIO, CTO, and Agency CIOs to help coordinate the recovery process.
- CTO – The CTO will be responsible for:
  - Working with the state CIO, Deputy CIO, Agency CIOs, and EMA's Director of the SEOC to coordinate the recovery process and to provide them with technical assistance in remediating the issues caused by incident(s).
  - Identifying critical assets that have been damaged or destroyed by the incident and forwarding the information onto the state CIO to request emergency purchase.
  - Ensuring that COOP Incident Command Team is contacted and briefed.
  - Ensuring that Agency Directors are briefed and they start making preparations to assist the COOP Incident Command Team.
  - Ensuring the COOP alternate facilities are prepped.
  - Ensuring that alternate communications are in place and operational.
  - Establishing networks and communication to alternate facilities that
- CISO – The CISO in conjunction with EISO will work with the state CIO and the CTO and assist with communications that identify the issues and the remediation efforts.
- EISO – At this level, the EISO is responsible for notifying agencies when the alert level changes from blue to yellow. In addition to this, the EISO will:
  - Incident Reports – The EISO will investigate incidents reported to them by the ISOs, Agency IT staff, or state employees.
  - Raising the Alert Level – The EISO will raise the alert level to orange and notify the state CIO Executive Management Team, state CIO SOS, state CIO EDC, Agency CIOs, and ISOs of the change and the reason for it.
  - Updating the EISO Cybersecurity Portal – The EISO will change the level on the cybersecurity portal and provide Local agencies and citizens with information about the threat and ways to avert it.
  - Remediation Efforts – The EISO will:
    - Continue recommended actions from previous levels.
    - Assist agencies with remediating the issues that are impacting their IT resources.
    - Assist EMA is establishing alternate forms of communication.
    - Closely monitor security mechanisms including firewalls, web log files, anti-virus gateways, system log files, etc. for unusual activity.
    - Consider limiting or shutting down less critical connections to external networks such as the Internet.
    - Consider isolating less mission critical internal networks to contain or limit the potential of an incident.
  - De-Escalation Process – The EISO will ensure that the issues that caused the alert level to be raised have been addressed before lowering the level back to blue.
- Telecommunications Service Provider SOC – The Telecommunications Service Provider will work with the EISO to help identify issues, block firewall ports, and assist with remediation efforts. The Telecommunications Service Provider may also be called upon to work with the EISO to reroute network traffic to systems that are not impacted by the cyber attack.

- The state EISO will identify and address potential cybersecurity incidents discovered by their security monitoring tools or reported to them by agencies, users, citizens, etc. In addition to this, the state CIO will do the following:
  - Incident Response – the state CIO will forward the EISO any cybersecurity related incidents reported to their 24/7 Hotline.
  - Enterprise Firewall Management – the state EISO will identify and block IPs that attacks are originating from.
  - Remediation Effort – the state CIO will designate team members to work with the EISO to remediate the issue(s).
- The state CIO EDC – the state CIO EDC will work with the EISO to identify the appropriate actions necessary to remediate the threat. In addition to this, the state CIO will:
  - Security Monitoring Tools – state CIO EDC will report any anomalies to the EISO.
  - PATCH Management – state CIO EDC will work with the EISO to identify the proper application patches and ensure they are installed on the servers that would be impacted by the threat.
  - Antivirus – state CIO EDC will ensure that all of the servers have the most current antivirus agents and files installed and that they are working correctly.
- State-CSIRT – State-CSIRT team members will be put on alert and they may be called upon to assist agencies in their remediation efforts.
- Agency CIO – The Agency CIO will work with their Deputy CIO and their Communities of Practice to address any concerns or issues; and to coordinate remediation efforts that may require assistance from the state-CSIRT, EISO, or other agencies within their Communities of Practice. Depending upon the event and its impact on the agency, the Agency CIO may need to activate it disaster recovery plan.
- ISOs – ISOs will work with their Agency CIO to help coordinate remediation efforts. In addition to this, ISOs will be responsible for:
  - Agency Alert Level – ISOs will be monitoring the incident and adjusting their Agency Alert level to properly match their readiness and remediation efforts.
  - Incident Reporting – ISOs are responsible reporting any incident that may come about during the remediation efforts or that may have caused the agency to raise its alert level.
  - Communication – ISOs will work with the Agency CIO, EISO, state CIO, state CIO EDC, Agency IT Staff, and their customers to identify and communicate information about the incident and remediation efforts.
- Agency IT Staff – The Agency IT Staff will work with the ISOs, EISO, state CIO, state CIO EDC to identify and remediate issues that are impacting their IT resources.
- Business Partners (BPs) and Service Providers (SPs) – BPs and SPs should reach out to their respective agency representatives to see if they need to assist in the remediation effort.
- GOHS – GOHS will reach out to their federal and local contact to apprise them of the situation and to determine if the event is isolated to the state or part of a larger attack being conducted by a nation state or cyber terroristic group.
- State CIC – The State CIC will work with law enforcement and DHS to determine if the event is criminal related. In addition to the criminal investigation, CIC may be called upon to help the with the remediation effort.

Red or Severe

At this level, unknown vulnerabilities are being exploited causing widespread damage and disrupting critical IT infrastructure and assets. These attacks are being felt at a national, state, and local level.

- Level Definition – At this level, malicious activity has been identified with a catastrophic level of damage or disruption. Examples include but not limited to:
  - Malicious activity results in widespread outages and/or complete network failures.
  - Data exposure with severe impact.
  - Significantly destructive compromises to systems, or disruptive activity with no known remedy.
  - Mission critical application failures with imminent impact on the health, safety or economic security of the State.
  - Compromise or loss of administrative controls of critical system.
  - Loss of critical supervisory control and data acquisition (SCADA) systems.



Actions:

- Continue recommended actions from previous levels.
- Contact MS-ISAC SOC for additional guidance.
- If this event is APT activity, steps other than the ones listed must be taken. Please contact the MS-ISAC SOC for guidance.
- Shutdown connections to the Internet and external business partners until appropriate corrective actions are taken.
- Isolate internal networks to contain or limit the damage or disruption.
- Use alternative methods of communication such as phone, fax or radio as necessary in lieu of e-mail and other forms of electronic communication.

- Escalation – In order to raise the state or agency threat level to Red, the following conditions must be in place:
  - Risk Level – The threat has the potential to impact multiple agencies and/or could require the state to shut down the IT infrastructure for six to thirty business days to restore normal business operations.
  - Impact to IT Services – At red, the following conditions are in place:
    - Impact
      - Telecommunications are unavailable making it necessary to use alternate forms of communication (radios, messengers, etc.).
      - The power grid is unreliable causing agencies to rely on the backup generators or UPS.
      - Buildings have been damaged or destroyed rendering IT resources inoperable.
      - State CIO Executive Staff have to relocate to EMA for command and control purposes.
      - COOP has to be implemented to restore IT operations.
      - Datacenters have to be restored or moved to their alternate facilities.
    - Time – The issues will take over ten business days to remediate and critical applications and services will be offline until the issues can be remediated.

    - Remediation Effort – The threat can only be remediated by restoring the applications, systems, and facilities to an operational state by either rebuilding equipment or restoring critical systems or applications to a previous date before the attacks occurred.
    - Agency Impact
        - Agency IT staff will work with state CIO to restore their equipment, systems, and applications to an operational state.
        - The Agency CIO will work with the DCIO, Office of General Counsel and Press Secretary to address any political or legal ramifications that may arise from the incident.
        - Cybersecurity EPLO may need to relocate to EMA and work with state CIO and their agency IT staff to restore IT Operations.
- Communication Procedures – At red the state's IT critical resources rendered inoperable by a cybersecurity that will take weeks to recover from. This event is impacting IT communications and necessitated the need for alternate forms of communications (satellite, radios, messengers, etc.).
    - State EMA – The state EMA will be notified via cell phone or messenger and they will enact their internal cybersecurity emergency response plan. In addition to this, the state EMA will:
        - Provide executive meeting and conference rooms for the CIO, CTO, and the DCIO to assist with the recovery process.
        - Establish temporary communications (Radio, Satellite, etc.) for recovery personnel.
        - Provide operational meeting and conference rooms for EPLOs and Agency IT staff assisting with restoring telecommunications.
    - MS-ISAC – After email communication is restored, EISO will contact MSISAC via email or telephone and request assistance with remediating the issue.
    - Fusion Center - provides advanced intelligence on current and emerging threats. As a threat increases in severity the fusion center will direct more resources toward monitoring the nature and behavior of the threat in terms of probability and magnitude of effects. The fusion center will notify stakeholders of its current assessment of the threat.
    - PA-ISAC – After email communication is restored, EISO will use email provide PAISAC members with an update or the share remediation data.
    - Cybersecurity Portal – Once the state's network is restored, EISO will use the cybersecurity portal to provide agencies and the citizenry with pertinent information.
    - E-mail – After it's restored, e-mail will be used to communicate alerts, status reports, updates, and ancillary information.
    - Telecommunications – after telecommunications are restored, land lines and cell phones will be used for clarification purposes and to address questions about remediation efforts.
- De-Escalation Criterion – In order to return to orange, the incident must meet the escalation criterion identified within that section.
- Responsibilities – When the state is at this level the following groups will be active and will carry out their assigned duties:
    - State CIO – At red, the state CIO will contact the Secretary of Administration to let him or her know about the severity of the situation. In addition to this, the state CIO will:
        - Activate COOP.
        - Relocate appropriate staff from the Secretary of Administration and Governor's offices to EMA for command, control, and communication purposes.

- Meet with Deputy CIO to talk about the contingency plans.
- Assist with the Secretary of Administration and Governor's office with crafting sensitive communications to politicians, media, etc.
- Assist with the Secretary of Administration contacting the Office of the Budget get emergency funding to replace equipment and resources damaged or destroyed by the event.
- Work with DGS to acquire alternate work sites for building and structures that are damaged or destroyed by the incident.

- DCIO – The DCIO will relocate to EMA to assist the state CIO, CTO, and Agency CIOs in the recovery process.
- CTO – The CTO will be responsible for:
  - Working with the state CIO, Deputy CIO, Agency CIOs, and EMA's Director of the SEOC to coordinate the recovery process and to provide them with technical assistance in remediating the issues caused by incident(s).
  - Identifying critical assets that have been damaged or destroyed by the incident and forwarding the information onto the state CIO to request emergency purchase.
  - Ensuring that COOP Incident Command Team is contacted and briefed.
  - Ensuring that Agency Directors are briefed and they start making preparations to assist the COOP Incident Command Team.
  - Ensuring the COOP alternate facilities are prepped.
  - Ensuring that alternate communications are in place and operational.
  - Establishing networks and telecommunications to OA/OIT and Agency alternate facilities.
- CISO – The CISO in conjunction with EISO will work with the CTO and assist with communications that identify the issues and the remediation efforts.
- EISO – At this level, the EISO is responsible for:
  - Incident Reports – The EISO be responsible for documenting what occurred and providing the CISO and CTO with a post mortem report.
  - Raising the Alert Level – The EISO will raise the alert level to red and be responsible for notifying the CIO's Executive Management Team, EDC, Agency CIOs, and ISOs of the change and the reason for it.

    Note: This may require the information to be communicated via a courier or a messenger service.
  - Updating the EISO Cybersecurity Portal – If the portal is available, EISO will change the level on the cybersecurity portal and use it to convey critical information.
  - Remediation Efforts – The EISO will:
    - Continue recommended actions from previous levels.
    - Assist agencies with remediating the issues that are impacting their IT resources.
    - Shutdown connections to the Internet and external business partners until appropriate corrective actions are taken.
    - Isolate internal networks to contain or limit the damage or disruption.
    - Use alternative methods of communication such as phone, fax or radio as necessary in lieu of e-mail and other forms of electronic communication.
  - De-Escalation Process – The EISO will ensure that the issues that caused the alert level to be raised have been addressed before lowering the level back to orange.

- Service Providers' SOC – Verizon will participate on any conference calls that the EISO sets up. In addition to this Verizon, will advise the EISO of any information from its business partners that could help restore the state's infrastructure.
- EDC – EDC will work with the EISO to identify the appropriate actions necessary to remediate the threat.
- State-CSIRT – State-CSIRT team members will assist agencies in their remediation efforts.
- Agency CIO – The Agency CIOs may need to activate their disaster recovery plan.
- ISOs – ISOs will work with their Agency CIO to help coordinate remediation efforts, and are responsible reporting any incident that may come about during the remediation efforts or that may have caused the agency to raise its alert level.
- Agency IT Staff – The Agency IT Staff will work with the ISOs, EISO, EDC to identify and remediate issues that are impacting their IT resources.
- CBPs – CBPs should reach out to their respective agency representatives to see if they need to assist in the remediation effort.
- GOHS – The Director of GOHS will join the CIO, CTO, DCIO, and critical infrastructure agency CIOs at EMA or a designated recovery site. During this timeframe, GOHS will continue to maintain communications with their federal and local contact to apprise them of the situation and communicate any information that the federal DHS may have about the event.
- CIC – The CIC Director will join the, CIC will join the EISO staff at EMA or a designated recovery site to help restore the state's critical infrastructure. In addition to this, CIC will work with local authorities to advise/assist them with the recovery process.