Planning Considerations for Cyber Incidents

Guidance for Emergency Managers

November 2023

FEMA

This page intentionally left blank.

Table of Contents

Introduction and Overview

1. Purpose

Emergency management personnel play a central role in preparing for and responding to cyber incidents in their jurisdictions.[1] Although emergency managers are not expected to be technical experts on cyber incidents, they do need to understand and prepare for the potential impacts of a cyber incident on their communities as well as on their emergency operations. Knowing whom to engage when a cyber incident occurs and having plans in place to effectively address an incident's impacts is central to the role of emergency managers, regardless of hazard type.

Developed by the Federal Emergency Management Agency (FEMA) in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), this guide is intended to help state, local, tribal, and territorial (SLTT) emergency management personnel collaboratively prepare for a cyber incident and support the development of a cyber incident response plan or annex. While focused on the roles and responsibilities that emergency managers in government may have, emergency managers in academia, nonprofits, or the private sector may also find the concepts helpful, especially if they serve on a jurisdiction's planning team.

1.1. Background

Nearly all aspects of society heavily rely on networked technologies. From phones and communications systems to home appliances and security systems, to transportation systems, medical systems, and utility services, nearly all aspects of society rely on networked technologies to communicate and operate. While increased interconnectedness provides better and more efficient services in many ways, the increasing reliance on technology and cyber connections may lead to cyber incidents with far-reaching and devastating impacts. An interruption in one organization or system, whether from a natural hazard, human error, equipment failure, or malicious attack, may have widespread impacts across a network. In the worst cases, this puts lives at risk and causes significant economic challenges. For these reasons, it is increasingly important that organizations and jurisdictions have a cybersecurity program in place to protect against disruptions and a cyber incident response plan in place to enable quick, effective resolutions when an incident occurs.

1.2. Cybersecurity and Cyber Incident Response

It is important to understand the difference and relationship between cybersecurity and cyber incident response. "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and

[1] CISA leads the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure. CISA also coordinates the execution of national cyber defense, leads asset response for significant cyber incidents and ensures that timely and actionable information is shared across federal and non-federal and private sector partners. For more information, visit CISA.gov/about-cisa.

availability of information."[2] The goal of cybersecurity is to stop or minimize disruptions. A cybersecurity program is designed to both understand and address cyber risks across an enterprise and is composed of people, processes, and technologies that monitor, detect and, ideally, prevent incidents on an ongoing basis. However, even with the best cybersecurity program in place, cyber incidents are always a risk. Therefore, it is important to have a cyber incident response plan or annex that enables organizations to act quickly. An effective and efficient response helps to mitigate impacts and return functional services as soon as possible. Much of cyber incident response planning occurs before an incident occurs and in conjunction with a cybersecurity program.

Although a fully mature cybersecurity program includes cyber incident response planning, effective planning for cyber incidents requires specific areas of focus. This guide provides considerations for cyber incident response planning, in line with the six-step planning process outlined in FEMA's Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining Emergency Operations Plans. It does not provide guidance for establishing a cybersecurity program or its protocols. There are many useful resources available to help organizations and jurisdictions set up and implement a cybersecurity program. Several key resources are highlighted below.

Resources for Building or Strengthening a Cybersecurity Program

- Cybersecurity Performance Goals: Provide baseline information technology (IT) and operational technology (OT) security practices that can improve resilience against, and meaningfully reduce the likelihood and impact of, known cyber risks and common tactics, techniques, and procedures (TTPs).
- Cyber Security Evaluation Tool (CSET): Provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. CSET includes the Cybersecurity Performance Goals Assessment, which organizations can use to evaluate their cybersecurity posture and drive investments towards meaningfully reducing the likelihood and impact of known risks and adversary techniques.
- National Institute of Standards and Technologies (NIST) Cybersecurity Framework: Provides strategic guidance to help build and execute a cybersecurity program. The framework helps organizations assess cyber risks and set plans for improving or maintaining their security posture.
- CISA Emergency Services Sector Cybersecurity Framework Implementation Guidance: Provides foundational guidance for how emergency services sector organizations may enhance their cybersecurity using the NIST Cybersecurity Framework.

In addition, understanding and managing cybersecurity risks are key to developing a strong program. The following resources can help organizations prioritize the most important activities:

[2] CISA, 2019, Security Tip (ST04-001), What is Cybersecurity?

- CISA Vulnerability Scanning: Provides automated vulnerability scans and delivers a weekly report, which helps secure internet-facing systems from weak configurations and known vulnerabilities.
- CISA Known Exploited Vulnerability (KEV) catalog: Authoritative source of vulnerabilities that have been exploited. Can be use by organizations to prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.
- CISA Emergency Services Sector Cybersecurity Initiative: Provides resources to help those in the emergency services sector better understand and manage cyber risks.
- CISA Cyber Essentials Starter Kit: Provides guidance for leaders of small businesses and small and local government agencies to help them start implementing organizational cybersecurity practices.
- CISA Free Cybersecurity Services and Tools: Identifies free cybersecurity tools and services to help organizations further advance their security capabilities.
- State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) Cyber Resource Compendium: Identifies some of the major references that may help build or strengthen an organization's cybersecurity program.
- Nationwide Cybersecurity Review (NCSR): Provides a no-cost, anonymous, annual self-assessment mechanism designed to measure gaps and capabilities of SLTTs' cybersecurity programs.

1.2.1. INTRODUCTION TO CYBER INCIDENT RESPONSE PLANNING

Cyber incidents, like other disruptive events, may have long-term unforeseen, cascading, and far-reaching consequences. The impacts may cause immediate consequences to a service or system, or indirect and cascading effects. Potential impacts are further complicated as cyber incidents may result from a variety of causes, such as a malicious attack, a natural disaster, human error, or equipment failure, each requiring distinct actions to resolve the situation. It may not be immediately known whether the root cause is cyber related. Emergency managers may be well into addressing the consequences of the event before realizing it is a cyber incident. For these reasons, cyber incident planning and response necessitate collaboration among emergency management, cyber professionals, law enforcement, private industry, and other key stakeholders.

Although incident response plans vary from organization to organization, their purpose is consistent: to enable effective and efficient response to a cyber incident, mitigate its impacts, and return services back to normal quickly. Having an effective cyber incident response plan in place before an incident occurs reduces the amount of time that organizations or jurisdictions spend determining who to contact, what to do, and defining ownership and responsibilities during the incident.

Incident response plans identify response team members and their backups, how to contact team members when an event is reported, and the roles of each team member. The plan outlines the steps taken at each stage of the process and designates the team member(s) responsible for each

step, as well as the team member charged with overall responsibility for the response. Cyber incidents create significant ambiguity, so it is important for planners to ensure that the plan developed is flexible and adapts to changing circumstances. More information on the planning process is provided in Appendix A and further detailed in CPG 101: Developing and Maintain Emergency Operations Plans.

Specific to cyber planning, there are different cyber incident response approaches that jurisdictions may leverage when developing a cyber incident response plan. The National Institute of Standards and Technologies (NIST)'s approach is one of the most respected. NIST's Computer Security Incident Handling Guide "assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively."

NIST's approach applies a four-phase incident response lifecycle, shown in Figure 1 and listed below.[3]

1. **Preparation:** Preparation is essential to both preventing and responding to a disruptive cyber event. In preparing for a cyber incident, NIST suggests implementing a series of tools ahead of time. This preparation provides the community with a framework to analyze, isolate, and respond to an incident. Development of a clearly articulated cyber incident response plan with established points of contact, before an incident occurs, is important to this preparation phase.
2. **Detection and Analysis:** The second phase is determining an incident has occurred, its severity, and its type.
3. **Containment, Eradication and Recovery:** The third phase focuses on addressing the identified incident. It includes containment—preventing the spread of the incident and limiting its impact, eradication—removing the cause of the incident, and recovery—restoring normal operations and recovering any data that may have been lost or damaged. During this phase, the incident response team often cycles back to detection and analysis to ensure all elements of the incident have been identified.
4. **Post-Incident Activity:** This phase focuses on identifying lessons learned and opportunities for improvement. By evaluating the response process and outcome, organizations can identify best practices and make necessary changes to prevent similar incidents from occurring in the future. They can also identify areas for improvement in incident response planning, communication, and overall incident management.

[3] NIST, 2012, *Computer Security Incident Handling Guide*, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

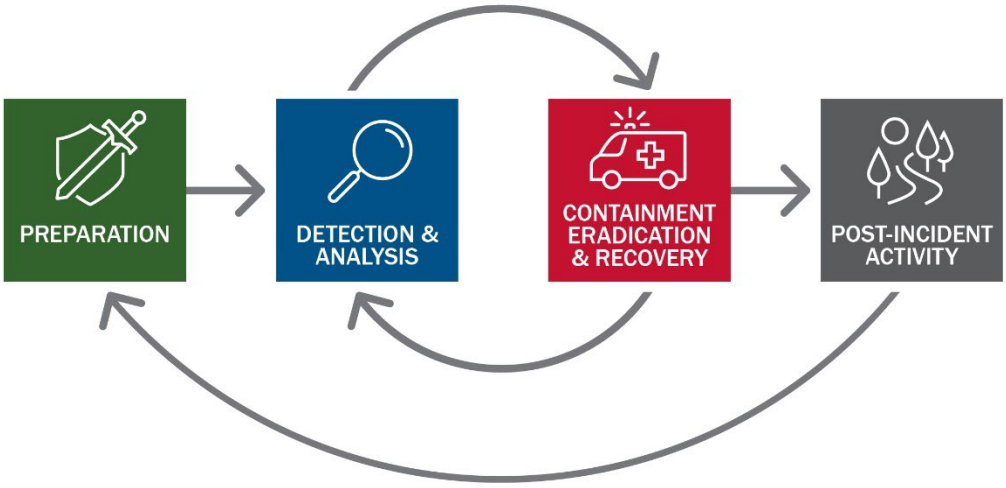

Figure 1: NIST Incident Response Lifecycle

Development of the incident response plan falls into the Preparation phase of the incident response lifecycle and will set the framework for executing the remaining phases when needed. Phases 2, 3 and 4 of the NIST incident response lifecycle are highly technical and require extensive cyber expertise. For this reason, it is essential that development of the cyber incident response plan is a collaborative effort among emergency management, cyber professionals, law enforcement, private industry, and other key stakeholders.

1.2.2. LEGAL CONSIDERATIONS

Emergency managers should consult with their legal advisors as they prepare for and respond to cyber incidents. Some jurisdictions already have specific laws or ordinances pertaining to cybersecurity and data protection, such as safeguards for personally identifiable data or cyber incident reporting. Although it mentions legal considerations, this document does not constitute or provide compliance or legal advice. This document is intended to be general guidance for a variety of factual circumstances, so readers should confer with their respective advisors to obtain advice based on their individual circumstances and applicable legal requirements.

2. Types of Cyber Incidents

A key step in planning for cyber incident response is identifying the types of cyber incidents that the jurisdiction may face. While it is not feasible to comprehensively identify all the specific cyber incidents that could impact an organization, it is important for emergency managers to have a general understanding of the common types of cyber incidents, along with the types of systems incidents may impact. Incidents may impact the OT/industrial control systems (ICS) that operate, control, and monitor industrial processes throughout U.S. infrastructure along with the associated IT systems. Owners and operators who understand cyber actors' TTPs can use that knowledge to prioritize hardening actions. Partnerships with other key personnel and subject matter experts help identify the types of incidents most likely to occur among these varying types of systems in the

jurisdiction and their immediate and cascading impacts. This foundational understanding of the common types of cyber incidents also helps with the development of incident scenarios that are useful to the planning process.

This section provides a general overview of key cyber concepts and incident types. It first describes the primary types of cyber assets and the role they may play in cyber incidents, then reviews the common causes of cyber disruptions. The content in this section is not intended to be all-encompassing. Please see the glossary for additional cyber terms and definitions.

Cyber Assets and Systems[4]

Assets are items of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation).

Systems are a combination of interacting elements organized to achieve one or more stated purposes. Interacting elements in the definition of system include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities.

Operational Technology (OT)/Industrial Control Systems (ICS) include a broad range of programmable systems and devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring or control of devices, processes, and events. ICS are an example of OT that control critical infrastructures.

2.1. Overview of Cyber Assets and Incident Types

Cyber assets include hardware, software, and networks. Hardware performs the physical functions, software directs and controls the hardware, and a network is a connection of computers enabling them to communicate and share information. Cyber assets range from systems with local networks to assets with internet access including smart phones, security systems, building management systems, heating and air conditioning systems, phone systems, smart home devices, vehicle control systems, and more. Identifying critical services in the jurisdiction and understanding how those services depend upon different types of cyber assets allows jurisdictions to assess how different types of incidents might affect their key functions. Impacts will often cascade, meaning that a particular impact on a specific system may be caused by an impact on an upstream system, or may cause further impact on a downstream system.

Below is an overview of three common cyber incident types. Although each is described independently, any of these incident types is likely to cause overlapping and cascading effects. The

[4] NIST, 2021, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

compromise of any hardware, software, or network is likely to result in the loss or degradation of services and may allow a malicious actor access to confidential information or system controls.

- **Hardware Destruction or Loss**: A jurisdiction's critical services often depend upon the hardware (e.g., computers, industrial control systems, storage devices, network infrastructure) that perform critical functions. This hardware may enable day-to-day community functions, such as controlling drinking water systems and water filtration, managing court processes, providing payment systems for municipal services, and controlling traffic safety systems. It also may support critical emergency services, such as 911 services and radio transmitters used to communicate among emergency personnel. The infrastructure that provides these services may be overlapping. Hardware damage may result in the loss of computer and network communication services as well as the loss of data and can disrupt critical services. Hardware destruction or loss can be caused by natural hazards including floods, fires, and tornados, as well as electricity surges resulting from natural phenomenon such as lightning or geomagnetic disturbances/storms. Damage can also be caused by malicious acts. The unusual loss of a controller can be a complex issue to investigate. Engineers may initially attribute the loss to equipment failure, but further examination may uncover that it was due to a malicious attack on the controller, where a threat actor has introduced malicious code or malware and caused a catastrophic failure of the controller. This can have potentially devastating consequences for the system, leading to extended downtime and disruption of operations. It is therefore essential to investigate any unusual losses of controllers and identify the cause to ensure the security of the system.

- **Network Unavailability, Compromise, Degradation, or Destruction**: Networks enable computers to communicate and share information. Most critical services rely on networks. Incidents affecting networks may occur because of both natural disasters and malicious attacks. Since many systems depend upon external organizations and are often provided by third parties, an incident affecting the jurisdiction may be the result of a third party's incident. The impact may vary from unreliable communication among computers to a complete loss of communication. Identifying how the jurisdiction uses networks helps the planning team to understand how the jurisdiction depends upon these systems and to evaluate the potential consequence of their loss.

- **Software Malfunction, Compromise, or Exploitation**: Incidents affecting software may cause the loss or compromise of critical functions. Most of these incidents are caused by human error or accidental misconfigurations. However, incidents affecting software may also result from malicious attacks. Malicious actors may steal confidential information, modify and violate the integrity of information, or deny access to information by encrypting it and demanding money (ransom) to decrypt it. Malicious actors may also exploit software to compromise the integrity of physical systems such as security cameras, water and wastewater treatment, dams, traffic signs and signals, streetlights, pipelines, and facility management, which are often controlled (or monitored) by computerized industrial control systems.

2.2. Overview of Incident Cause

In most cases, determining the cause of a cyber disruption requires extensive cyber expertise. It is often unclear at the beginning of an incident whether the effects are caused by a malicious actor or another source, and it may take days or months to determine. The information in this section is not intended to help identify the cause of a particular incident. Rather, it is intended to highlight the primary causes of incidents to help the planning team think through potential cyber incidents that may occur in their jurisdiction, whether the result of natural hazards, accidents, or intentional attacks.

2.2.1. NON-MALICIOUS INCIDENTS

Non-malicious cyber incidents happen for numerous reasons. NIST includes the following non-malicious causes when categorizing threat sources: human errors, structural failures of organization-controlled resources (e.g., hardware, software, environmental controls), and natural and human-caused disasters, which are accidents and failures beyond the control of the organization.[5]

- **Human Error**: Cyber incidents may be caused by accidental errors made by individuals while performing their regular responsibilities. For example, mistakes happen while performing administrative tasks, such as installing or configuring hardware and software or conducting maintenance of computers and networks. These unintentional errors cause incidents that disable, disrupt, or damage computers, networks, and information.

- **Structural Failures**: These incidents happen when hardware, software, or support systems, such as environmental controls (e.g., air conditioning), fail. Hardware and software often contain unknown flaws that appear unexpectedly. These flaws may cause incidents ranging from loss of services to the loss or corruption of important information. When computing or networking demands exceed the capacities of the cyber resources, the cyber services might stop operating, corrupt or lose important information, or create other problems.

- **Natural Disasters**: All types of cyber assets depend upon physical systems ranging from hardware for computers and networks to the infrastructure that manages operational environments. Natural disasters and accidents may damage or disrupt the operation of physical systems. Fires, floods, windstorms, and electrical disturbances often cause non-malicious cyber incidents. Loss of electrical power is another common cause. Uninterruptible power supplies handle short-term power problems, and alternative power generation systems such as diesel generators handle long-term losses, provided fuel is available.

[5] NIST, 2012, *Guide for Conducting Risk Assessments*, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf.

2.2.2. MALICIOUS INCIDENTS

Malicious actors attempt to compromise the availability, integrity, or confidentiality of computers, networks or information. As noted above, the specific cause of an incident will rarely be known while the event takes place. More often, it is discovered days or months later following a forensic examination of the impacted equipment or software.

- **Denial of Service (DoS)**: DoS attacks flood computers and networks with traffic that overloads a network and disrupts legitimate requests. Such traffic often originates from multiple locations to complicate attempts to block them and may serve to amplify the malicious traffic directed at the targeted computers. These are described as distributed denial-of-service (DDoS) attacks. By limiting access to websites used for business operations, malicious actors may cause a variety of issues, including financial losses or damage to the reputation of businesses. Similarly, malicious actors have used DDoS attacks to deny access to government websites.

- **Malware**: Malware is a broad term for any type of malicious software designed to harm or exploit a programmable device, service, or network. Malware appears in various forms and may perform a wide variety of malicious actions:

    - Ransomware uses encryption to deny access to information. Ransomware actors demand ransom to decrypt the information and may also threaten to publish the information unless the ransom is paid.

    - Spyware infects computers and collects information about user activity, such as usernames and passwords, payment information, information in emails, and other sensitive information that may enable threat actors to perform other malicious activity.

    - A trojan provides a backdoor gateway for malicious programs or threat actors to enter a system and steal valuable data without the user's knowledge or permission.

    - A worm replicates and spreads across devices within a network. As it spreads, it consumes bandwidth, overloading infected systems, and making them unreliable or unavailable.

A common delivery method for cyber intrusions is **Phishing**. Malicious actors use phishing attacks to steal sensitive information and potentially enable malicious access to a computer or system. Phishing is typically conducted through email or text messages (smishing) to trick people into clicking a link, downloading malicious software (malware) or revealing login credentials. If successful, phishing may infect the email recipient's computer. Spear phishing is a tactic that targets specific organizations or individuals with personalized messages that deceives the receiver into trusting the message. For more information about phishing, see CISA's guide on Phishing Guidance: Stopping the Attack Cycle at Phase One.

- **Third-Party Compromises and Supply Chain Attacks**: Malicious actors attack third-party vendors of software and services because other organizations rely upon and trust vendors and

install their software to manage complex systems. Adversaries gain access to third-party vendor software to exploit the modified software once installed by the vendor's customers.

3. Assessing Cyber Risks to Inform Prioritization and Planning

Effective preparedness for cyber incidents requires that jurisdictions understand how essential services and infrastructure in the community, including emergency management services and infrastructure, rely on cyber systems and the potential cascading impacts of a disruption. This knowledge helps the jurisdiction's planning team determine response actions and resources that are needed in a cyber incident, as well as how to prioritize restoration efforts.

3.1. Engaging Service Owners and Operators

Owners and operators of critical services and their associated cyber systems play an important role in preparing for cyber incidents, including assessing cyber risks. The owners and operators provide the most detailed and accurate information regarding system dependencies and vulnerabilities and valuable guidance on assessing whether the service remains operational during and following an incident. Engaging owners and operators in assessing cyber risks and planning for cyber incidents also helps establish relationships with cyber staff and service providers. These relationships foster a shared understanding of vulnerabilities and impacts related to specific incident types and aid in the development of effective plans, policies, procedures, and protocols.

Engagement with owners and operators of critical services and cyber systems is essential to successful cyber incident response planning. However, some organizations may be reluctant to collaborate due to concerns such as sharing proprietary information, the risk of data leakage, and the potential for brand and financial damages in the event of an incident. Establishing a confidentiality agreement, Non-Disclosure Agreement (NDA), private-public partnership, or other legal agreement in consultation with appropriate legal advisors may reduce these concerns. FEMA's Building Private-Public Partnerships Guide[6] provides best practices for building and maintaining these partnerships.

[6] FEMA, 2021, *Building Private-Public Partnerships*, https://www.fema.gov/sites/default/files/documents/fema_building-private-public-partnerships.pdf.

Cyber Asset Owners and Operators

Asset owners are people or organizational entities, internally or externally, that have primary responsibility for the viability, productivity, and resilience of the asset.

Asset operators are people or organizational entities, internally or externally, who are responsible for satisfying the protection and sustainment requirements for the asset established by the asset owner. Asset operators include system/database administrators, industrial control system engineers, facility managers, IT support organizations, and contractors who host and manage data (e.g., cloud service provider).

3.2. Assessing Cyber Risks

Assessing cyber risks enables the jurisdiction to identify the most likely cyber disruptions with the most severe impact for their community. This aids the jurisdiction in identifying the response actions and resources needed in a cyber incident, as well as how to prioritize restoration efforts. Assessing cyber risks requires the following actions:

- Identifying the critical services for the community that rely on OT and IT, such as emergency services, water and wastewater systems, and communications.
- Identifying the dependencies of critical infrastructure, particularly those related to critical services, cyber assets, and services.
- Identifying the consequences of service loss or disruption, with special attention to the problems caused by cyber incidents.

Developing a critical services and dependencies inventory is a good way to identify, examine, and document this information. The inventory captures the critical services, infrastructure, assets, associated owners and operators, other key personnel, and the dependencies among systems. In addition to helping with this assessment and prioritization process, this inventory may also be included within the cyber incident response plan or annex for reference during an incident.

3.2.1. IDENTIFYING CRITICAL SERVICES

Identifying the jurisdiction's critical services that rely on cyber systems is the first step in the assessment process. The planning team begins by identifying the known critical services and their owners and operators, then expands to identify other related services. This helps build the critical services and dependencies inventory. It also provides an opportunity to identify additional key stakeholders to include in the planning team (see Appendix A for information on the six-step planning process and for more guidance on forming the core and collaborative planning teams).

When identifying critical services, it may be beneficial to use community lifelines[7] as a starting point. Community lifelines are services that enable the continuous operation of critical government and business functions and are essential to human health and safety or economic security. They are the most fundamental services within a community that, when stabilized, enable all other aspects of society to function.

Continuity of Operations Planning

Continuity is the ability to provide uninterrupted critical services, essential functions, support, and other priority services while maintaining organizational viability, before, during, and after an event that disrupts normal operations.

It may be helpful to consider continuity planning best practices when establishing and updating cyber incident response plans. Cyber incidents may result in degraded communications, compromised systems, or inoperable facilities. It is crucial that jurisdictions' continuity assessments and plans include cyber considerations.

For more information on continuity planning, assessment tools and resources, visit: Continuity Resources and Technical Assistance at fema.gov.

3.2.2. IDENTIFYING SERVICE DEPENDENCIES

Identifying and understanding dependencies among systems and assets helps the planning team, and ultimately the incident response team, consider what may disrupt key services or other assets on which those services depend.[8] It also helps to identify the upstream or downstream implications. This process helps the planning team anticipate possible impacts to community lifelines, which may influence the prioritization of incident response decisions and actions.

Using the list of critical services and their owners and operators as a starting point, the planning team identifies service dependencies by:

- **Engaging with Service Owners and Operators:** The service owners and operators provide key information about the system to assist with building an understanding of the jurisdiction's dependencies.
- **Identifying and Engaging Other Stakeholders of Each Service:** Some services involve additional stakeholders beyond the system owner such as security professionals, third-party service providers, or a cyber incident response team (CIRT). Understanding all the stakeholders and their roles aids in identifying who is contacted when an incident occurs.
- **Identifying Support Contacts for All Vendors and Contracted Service Providers:** Not all services and systems are owned, serviced, or maintained by in-house staff. As a result, third-

[7] For more information on community lifelines, visit: https://www.fema.gov/emergency-managers/practitioners/lifelines.
[8] For an overview of dependencies, visit: https://www.cisa.gov/what-are-dependencies.

party or support contacts may need to be part of the planning effort. The planning team works with service owners to identify any support contracts and determine what these contracts may provide during an incident. For example, the internet service provider may help identify the type of attack and potentially block the attacker if requested.

As the planning team identifies and documents the dependencies in the critical services and dependency inventory, considerations include:

- **Upstream Dependencies:** These are products or services provided to a jurisdiction by an external organization that are necessary to support its operations and functions. Examples of upstream dependencies include:
  - Supply of electricity from an electric utility distribution substation;
  - Telephone communication services;
  - Access to the internet; and
  - External organizations, such as a vendor that maintains essential software systems.
- **Internal Dependencies:** These are the interactions among internal services, operations, functions, and information of the jurisdiction. Examples of internal dependencies include:
  - Information services, such as websites, depend upon database servers;
  - Operational control systems depend upon process measurement systems; and
  - Computer systems depend upon computer network equipment.
- **Downstream Dependencies:** These are services provided by a jurisdiction to its residents or other jurisdictions. Examples of downstream dependencies include the ability to provide critical functions such as issuing death and birth certificates, deeds for property sales, 911 services, elections, drinking and wastewater treatment, traffic control, information services, scheduling portals, registration services, and customer billing.

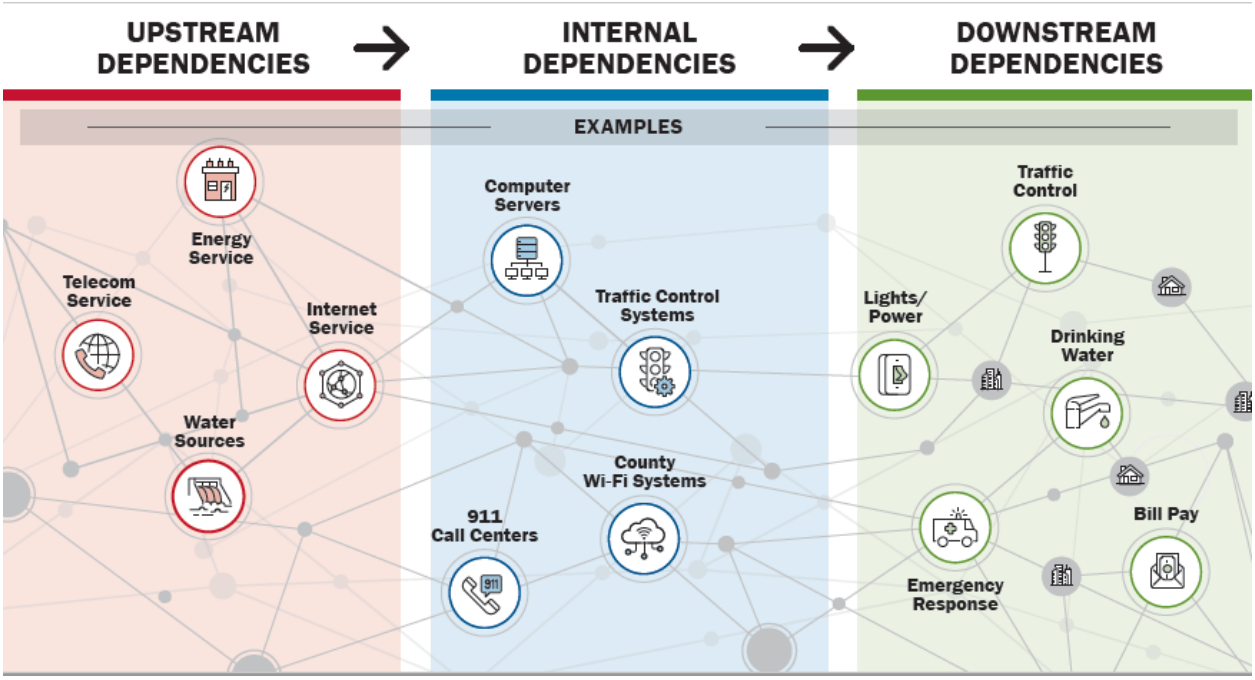

Figure 2: Examples of Upstream, Internal, and Downstream Dependencies

Questions to Assist in Identifying Dependencies

1. What are the service's external dependencies?

An external dependency exists when an outside entity (e.g., contractor, customer, service provider) has access to, control of, ownership in, possession of, responsibility for, or other defined obligations related to the critical service or its associated assets.

Examples of services provided to an organization from external entities may include: outsourced activities that support operation or maintenance of the critical service; security operations; IT service delivery and operations management or services that directly affect resilience processes; backup and recovery of data, provision of backup facilities for operations and processing and provision of support technology or similar resilience-specific services infrastructure providers such as power and dark fiber; telecommunications (e.g., telephony and data); technology and information assets (e.g., application software, databases); and education and training resources.

2. Which external dependencies are most important?

The intent of prioritization is to ensure that the jurisdiction properly directs its resources to the external dependencies that most directly impact the critical service.

Prioritization criteria may include dependencies that: directly affect the operation and delivery of the critical service; support, maintain, or have custodial care of critical service assets; support the continuity of operations of the critical service; save access to highly sensitive or

classified information; support more than one critical service; supply assets that support the operation of a critical service; or impact the recovery time objective of the critical service.

3. On which infrastructure providers does the critical service depend?

Critical services may be dependent on infrastructure providers to remain viable. The organization may need to address the loss of these providers, which may affect the resilience of the critical service. The jurisdiction may need to consider the resilience of the providers when developing service continuity plans.

These infrastructure services may include telecommunications and telephone services, data and network service providers, electricity, natural gas and other energy sources, and water and sewer services.

Considering Cyber Dependencies

When identifying dependencies for critical services, it is important to consider the interconnected nature of the service and its components. Cyber dependencies exist both internally and externally to an organization and may be through direct or indirect relationships. For example, websites depend upon servers, data, and access to the internet. Jurisdictions might provide and maintain their own software, computers, and networks to operate their websites, which form an internal dependency, or contract with external website providers to manage their websites, forming an external dependency. External dependencies often exist when jurisdictions contract with external organizations to provide services such as computer support and security. A direct dependency exists between a utility control computer and a computerized sensor, while a logical but indirect dependency exists between natural gas delivery systems and their customer billing systems.

Questions to Consider when Identifying the Owner of a Cyber System

- What part(s) of the jurisdiction is responsible for the delivery of the critical service?
- Who are the owners of the assets required for delivery of the critical service?
- Are both owners and operators of assets documented?

3.2.3. IDENTIFYING THE CONSEQUENCES OF SERVICE LOSSES OR DISRUPTIONS

With an understanding of key dependencies, the planning team may identify the likely consequences of service interruptions caused by the loss or disruption of another service or cyber asset. As part of this process, it is important to determine whether the consequence would occur immediately after an incident or later. For example, a service might fail immediately if its industrial control computer failed because of an attack or system fault. Or, a service might fail after the depletion of a resource, such as a backup battery providing power during a power outage. Awareness of these consequences, and associated impacts to community lifelines, helps to establish incident response priorities and identify

resources and capabilities that improve incident response and reduce the consequences of cyber incidents.

During this process, the planning team works with service owners and operators to understand the criticality of their dependencies on other services and cyber assets. This helps to identify the impact of the loss or disruption of these support services and cyber assets. In a cyber incident, cascading impacts are likely.

Sample Questions to Consider – Consequences of Service Loss or Disruption

- What happens if there is a sudden loss of access to servers with a municipality's email and contact data?
- What happens to the community water supply if the pumps lose electricity?
- What happens to the availability or quality of water if the industrial control systems or their communication networks are disrupted?
- What happens if the water treatment process is compromised by a malicious incident and the monitoring system is unable to show trustworthy, accurate testing results to human workers?
- What public health impacts may occur from the cyber incident? Are local healthcare facilities able to respond on a community-wide scale?
- What is the consequence if web-based services, such as scheduling and bill-payment, are unavailable because of a cyber incident that affects the computers or the network?
- Do impacted systems belong to a private company or a public entity?
- Are privately owned systems part of the critical infrastructure for the jurisdiction?
- What happens if financial information, such as customer credit card information, is stolen by a malicious actor?

As part of this process, the planning team may also determine how to gain situational awareness of the status and operational readiness of critical services during an incident so that information may be factored into plan development. Gaining this situational awareness will often depend on the managers of those services and cyber assets. While some services, such as water and electricity supply, are directly observable and customers will likely report losses, other services and cyber assets require the use of instruments that monitor and report on status. Additionally, service assessments might require personnel to check and report on operational readiness and whether services are affected by the cyber incident. The planning team engages with the owners and operators of critical services and assets to understand how status is monitored and communicated. This information is essential to the incident response, as it enables the emergency management team to understand what and how services are affected, what services are not affected, and what services might be affected later.

Planning ahead to quickly obtain information in a response may include:

- Establishing a partnership with a neutral, third-party intelligence organization (e.g., state/local fusion center, Multi-State Information Sharing and Analysis Center [MS-ISAC]);
- Establishing legal agreements among critical service providers to promote information-sharing; and;
- Creating anonymous reporting tools that scrub sensitive information while promoting shared visibility of the event or its impacts.

3.3. Prioritizing and Planning

Using information gained in the assessment process and documented in the critical services and dependencies inventory, the planning team appraises each cyber asset to determine how vital it is for the operation of critical services. The planning team, in close collaboration with the system owners and operators, discusses what redundancies or backups are available for those services if internet or web service connectivity is lost for a significant period of time. For example, some IT services may be able to be run manually or be relocated to a non-impacted location. Once these contingencies have been established, the planning team has a clearer understanding of what systems are essential, what is required to operate those systems, and what alternative methods are available for operating those services. The planning team uses this information to establish priorities for services, how to apply limited resources, and the order of response efforts prior to an incident.

The ordering of response efforts considers time-dependent aspects such as how long a service may remain unavailable or disrupted before causing a negative impact. During a response, the priorities may change rapidly as services become available or unavailable. These changes may indicate destabilization of community lifelines and be tracked and included in incident reporting products that support the reevaluation and determination of incident response priorities.

Cyber Risk Assessments Resources

- CISA Cyber Resilience Review Asset Management: Provides guidance on how to identify, document and manage assets to evaluate and improve cyber resilience and response.
- CPG 201: Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide: Provides guidance on conducting THIRA and SPR assessments and evaluating levels of preparedness.
- FEMA National Risk and Capability Assessment: Provides guidance for assessing the risk of all threats and hazards.
- NIST Guide for Conducting Risk Assessments: Provides guidance for assessing cybersecurity risks of federal information systems and organizations.

4. Emergency Management Roles and Responsibilities

Emergency managers' roles and responsibilities in preparing for and responding to a cyber incident may differ from those associated with other incident types. Roles and responsibilities may also differ across jurisdictions based on existing authorities and plans. Some jurisdictions place the emergency management organization in the lead coordinating role for cyber incidents, while others identify IT or law enforcement entities as the primary coordinator. In those instances where emergency management is not the lead, emergency managers take on supporting roles focused on the consequence management related to impacts from the incident.

In many jurisdictions, the emergency manager is responsible for coordinating the development of a plan or annex focused on cyber incident response, and for factoring cyber considerations into other plans. This often includes the oversight and leadership of the planning team and ensuring the necessary representatives are engaged in the effort. See Appendix A for guidance on forming the core and collaborative planning teams, including cyber-specific considerations.

Emergency managers should understand the stages of a cyber incident (described in the Introduction to Cyber Incident Response Planning section of this guide and NIST's Computer Security Incident Handling Guide), as well as the relevant legal requirements or restrictions and the roles and responsibilities that are listed in the jurisdiction's cyber plan or annex, if available. Beginning with detection of a cyber incident, emergency managers have important responsibilities in the management of direct and indirect impacts. Similar to other technical hazards, emergency managers may not be expected to directly work on containing and eradicating cyber threats. To the greatest extent possible, response actions taken should avoid causing further damage or impacts to threat investigation and removal operations by cyber professionals. Emergency managers may also assist with communication procedures including notifying the appropriate people. They may also be able to help manage questions throughout an incident to ensure that timely remediation occurs for the affected organization. As the focus of the incident transitions to recovery[9], emergency managers coordinate with the cyber response team to verify that the threat is contained and with stakeholders to ensure that affected operations are restored.

During an incident, emergency managers prioritize resources, such as personnel, to address the needs of response. Depending on impacts of an incident, emergency managers may activate other plans (e.g., power outage, distribution management). Activation of other plans may require incorporation of additional partners into incident support and consequence management. While not required of SLTT agencies managing cyber incidents within their own jurisdiction and capabilities, supporting federal lines of effort helps to ensure a robust response[10]. Balancing these potentially

[9] For more information visit the NIST Guide for Cybersecurity Event Recovery at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf.

[10] For more information on cyber incident identification and reporting, visit Appendix B: Cyber Incident Identification and Closing Processes.

competing operational demands and the potential for cascading effects on stakeholders may require the establishment of a unified coordination structure.

Unified Coordination Group (UCG)

A Unified Coordination Group (UCG) is the primary organizational structure for managing and supporting complex disaster response operations. Depending on the needs of the incident, a UCG is comprised of senior leaders representing jurisdictional interests and may include federal, state, local, tribal, or territorial governments; the private sector; or nongovernmental organizations. In coordination with applicable government and private entities, Emergency Support Function personnel assess the situation and identify requirements. Federal agencies may provide resources under mission assignments or their own authorities. The UCG applies unified command principles for coordinating the assistance provided to support the jurisdiction's response.

For instance, in 2016, Presidential Policy Directive on United States Cyber Incident Coordination (PPD-41, July 2016)[11] established lead federal agencies and an architecture for coordinating the broader federal government response to cyber incidents. PPD-41 created the Cyber UCG to serve as the primary coordinating structure among federal agencies in response to significant cyber incidents, as well as the integration of private sector partners into incident response efforts, as appropriate. The lead federal agencies for this UCG are the Department of Justice (acting through the Federal Bureau of Investigation), the Department of Homeland Security (acting through CISA) and the Office of the Director of National Intelligence. When cyber incidents threaten or result in physical consequences leading to a Stafford Act declaration, FEMA may serve in a combined Cyber/Physical UCG. Guided by the specific needs of an event, the Cyber UCG may involve additional federal agencies, SLTT governments, non-governmental organizations, international counterparts, and the private sector.

Considering the complex nature of cyber incidents and the high potential for cascading impacts, jurisdictions of all sizes may consider using a UCG structure to better organize response and recovery efforts to ensure that the priorities of various officials, subject matter experts, and asset owners are consistent and best meet the needs of the incident.

Emergency managers rehearse their roles and responsibilities for cyber incident response through customized scenarios and exercises. Such activities help the planning team explore contingencies, identify gaps, validate existing plans, and determine appropriate courses of action. Activities are iterative and build on prior incidents and exercises to strengthen jurisdictional capabilities. The incident examples below may be used to identify potential lead and supporting roles for emergency managers.

[11] Presidential Policy Directive on United States Cyber Incident Coordination, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

Example Scenario #1: Compromised Water Systems

Early on the morning of November 5, 2020, a water treatment facility within Central City received a call from a customer complaining about their water: "I went to get some water from my kitchen sink, and it immediately smelled like bleach was coming out of the faucet. It tasted wrong, even after I tried boiling it for my morning coffee. Is it safe to drink the water?"

An inspector performs a manual measurement of the chlorine levels in the water system and verifies that the water contains too much chlorine. The investigation includes an examination of the control system that operates and monitors the water treatment process. The control system displays the settings that regulate the release of chlorine and monitor the levels of chlorine appear normal. All physical controls (e.g., gates, locks) are operating as expected.

The facility's IT department suspects a cyber actor tampered with the technical controls to release an abundance of chlorine but need time to verify their theory and to hire additional forensic professionals. They aren't ready to release information to staff or the press until they can confirm the source. The water treatment department issues a "Do Not Drink" Water Advisory to inform their customers that the water is contaminated with potentially harmful amounts of chlorine and boiling the water does not make it safe to drink.

Example Emergency Manager Lead Roles:

- ☐ Coordinating communication to identify the scope of the incident (e.g., what jurisdictions are impacted)
- ☐ Activating the emergency operations center
- ☐ Developing Incident Action Plans
- ☐ Coordinating with cyber authorities to maintain situational awareness and reporting
- ☐ Managing coordination of resource and support requests from responding agencies
- ☐ Organizing hazardous materials support to identify and secure contaminated areas
- ☐ Identifying the potential for cascading impacts or additional hazards following the incident
- ☐ Tracking capability gaps and strengths for improvement planning following the incident

Example Emergency Manager Supporting Roles:

- ☐ Communicating information about the incident to law enforcement and nearby jurisdictions
- ☐ Developing and distributing notifications to the public regarding impacts and status
- ☐ Coordinating safety and security of the impacted property, as necessary
- ☐ Engaging private sector partners to provide resources and technical support
- ☐ Coordinating the distribution of emergency supplies of potable water

Example Scenario #2: Tornado

Late in the evening of June 20, 2022, Central City experienced an intense thunderstorm that quickly intensified. Meteorologists issued a "Tornado Watch," and shortly after a "Tornado Warning" circulated throughout Central City. Within minutes, an EF-4 tornado touched down and caused widespread, severe damage to property and infrastructure. The tornado caused widespread electricity outages and the heavy rainfall caused widespread flooding.

Preliminary damage assessments indicate that several buildings that provide critical services for Central City were damaged by the tornado and their contents appear to have been exposed to the rain. These buildings house computer and communications systems that serve the jurisdiction. These cyber systems — computers, networks, and communications gear — may have suffered physical damage from the tornado, water damage from the rain, or electronic damage from lightning. Response teams are struggling to establish communications and coordination due to power outages and disruptions to communications systems in the area.

Example Emergency Manager Lead Roles:

- ☐ Activating pertinent emergency operations plans and/or annexes
- ☐ Advising senior officials regarding the situation and emergency/disaster declarations
- ☐ Identifying incident objectives and priorities in coordination with jurisdictional leadership
- ☐ Activating the emergency operations center
- ☐ Developing Incident Action Plans
- ☐ Assessing the storm's impact on the jurisdiction's critical services
- ☐ Communicating with the public about the status of key critical services and safety risks
- ☐ Coordinating response to and recovery from the loss of critical services
- ☐ Coordinating temporary emergency power at critical facilities and alternate communication resources needed for key services, such as 911 call centers
- ☐ Identifying the potential for cascading impacts or additional hazards following the storm
- ☐ Serving as a coordination point for response partners, supporting communication, incident command, and the development of a common operating picture
- ☐ Tracking capability gaps and strengths for improvement planning following the incident

Example Emergency Manager Supporting Roles:

- ☐ Providing situational awareness reporting
- ☐ Coordinating safety and security for impacted property, as necessary
- ☐ Coordinating with third-party vendors or suppliers with impacted property

Example Scenario #3: Insider Threat

While employed with Central City's publicly owned Power & Electric (P&E) Company, a billing specialist had administrator access to the computer systems used by city residents to pay gas and electric bills online. In early July 2021, the billing specialist was terminated from P&E, losing access to the company's computer systems. The billing specialist was irate over the termination, arguing that it was unfair and unjust. After receiving a final paycheck, in retaliation for the termination, the former employee used a fake user account that had previously been created while employed with P&E to log into the company's computer systems.

Once logged in through the fake user account, the former employee created a second fake user account and used it to edit approximately 50,000 records and delete approximately 1,000 records. Of particular concern, the former employee changed the accounts of numerous residents to appear that they were months delinquent in paying their utility bills, resulting in thousands of residents and businesses having their electricity incorrectly turned off. The edits and deletions are also disrupting the ability of city residents to pay their bills online. After taking these actions, the former employee deactivated both fake user accounts and logged out of the system.

Example Emergency Manager Lead Roles:

- ☐ Coordinating with P&E to maintain situational awareness and reporting
- ☐ Identifying the potential for cascading impacts or interruptions to the community's essential services
- ☐ Activating the emergency operations center
- ☐ Developing Incident Action Plans
- ☐ Tracking capability gaps and strengths for improvement planning following the incident

Example Emergency Manager Supporting Roles:

- ☐ Communicating information about the incident to law enforcement and nearby jurisdictions
- ☐ Developing and distributing notifications to the public regarding impacts and status
- ☐ Determining what activities are needed to support residents who have lost power, including those who are dependent on electricity for life sustaining medical needs
- ☐ Coordinating with mass care organizations to provide assistance to residents in the event that power restoration is delayed
- ☐ Engaging private sector partners to provide resources and technical support
- ☐ Coordinating the distribution of emergency resources, such as generators, as necessary

5. Communication Considerations

Communications during cyber incident response need to be carefully planned, and similarly to communication considerations for other incidents, include both information sharing among emergency management and incident response personnel, as well as messaging out to broader stakeholder groups and the general public. This section presents key considerations for communicating before, during, and after a cyber incident.

5.1. Integrated Communications

It is important to identify who will serve as the lead for communications in a cyber incident and how the communications will occur. As described in the National Incident Management System (NIMS), integrated communications are a foundational characteristic of incident command and coordination. "Integrated communications provide and maintain contact among and between incident resources, enable connectivity between various levels of government, achieve situational awareness and facilitate information sharing. Planning, both in advance of and during an incident, addresses equipment, systems, and protocols necessary to achieve integrated voice and data communications."[12] Impacts from cyber incidents may adversely affect voice and data communication channels, either by taking them down entirely or comprising the security of the system, necessitating alternative communication channels. Planning efforts consider and address reporting mechanisms for cyber incidents, the possibility of degraded communications, notification procedures for key stakeholders, and handling procedures for sensitive information.

- **Reporting:** The planning team identifies who is contacted in the event of a cyber disruption, what details are reported, and how that information is reported. Consideration is given to when the cyber incident should be reported to CISA. CISA encourages voluntary reporting. Consideration should also be given to when law enforcement is notified, such as if criminal activity is suspected or an act of cyber terrorism (cyber events that impact critical infrastructures), federal reporting processes, and any legal requirements related to notification.[13] For cyber incidents that may be malicious, it is best to ensure the reporting channel is outside the affected systems. For example, an organization that believes their systems are compromised would not use email. Instead, they might utilize a phone unaffiliated with the organization to ensure that their communications are not intercepted by the malicious actor.

- **Alternative Communications Systems**: Cyber incidents, regardless of cause, may render common voice and data communications channels unusable. It is important for the planning team to understand how their communication channels rely on cyber systems and how they may be impacted. The planning team identifies alternative communication mechanisms to use when needed and ensures all appropriate parties have the knowledge and access to effectively use

[12] National Incident Management System, Third Edition, October 2017.

[13] For more information on cyber incident identification and reporting, visit Appendix B: Cyber Incident Identification and Closing Processes.

those channels. For cyber incidents that may be malicious, responders identify communication channels that are separate from the impacted platform since threat actors may intercept sensitive information on compromised channels. CISA recommends developing and implementing a Primary, Alternate, Contingency, and Emergency (PACE) plan, which establishes options for redundant communications capabilities if an incident disrupts or degrades primary capabilities.[14]

- **Notification of Key Entities**: The planning team establishes procedures for identifying which stakeholders to notify in the event of a cyber incident (or how to determine which stakeholders to notify) and what information to communicate. It is best to pre-identify points of contact for communications, both internally and with key external partners. Aligning communications to the content required per CISA's incident reporting form and other key information may include:
  - Date of the incident;
  - Description of the incident;
  - Processes or services affected by the incident;
  - Actions taken so far to deal with the incident;
  - Any actions that the stakeholder may need to take; and
  - Contact information to receive further information.
- **Information Sharing**: As discussed in Engaging Service Owners and Operators section of this guide, communications before and during a cyber incident may require the sharing of sensitive information, necessitating the establishment of a confidentiality agreement, NDA, or other legal agreement such as a private-public partnership. Ideally, such an agreement is established before an incident occurs, though in some instances they may need to be developed during incident response. The planning team considers such requirements when developing their plan or annex and includes a procedure for quickly establishing such agreements when an incident occurs.

[14] For more information on Primary, Alternate, Contingency, and Emergency (PACE) planning, visit: https://www.cisa.gov/sites/default/files/2023-05/23_0426_ncswic_PACE-Plan_508.pdf.

National Emergency Communications Plan

The National Emergency Communications Plan (NECP) is the Nation's strategic plan to strengthen and enhance emergency communications capabilities. Its vision is to enable the Nation's emergency response community to communicate and share information securely across communications technologies in real-time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event.

The NECP establishes six strategic goals to drive progress toward the vision: Governance and Leadership; Planning and Procedures; Training, Exercises, and Evaluation; Communications Coordination; Technology and Infrastructure; and Cybersecurity. By adopting these goals, public safety organizations support three national priorities for advancing emergency communications: enhancing effective governance among partners with a stake in emergency communications, addressing interoperability challenges posed by rapid technology advancements and information sharing, and building a resilient and secure emergency communications systems to reduce cybersecurity threats and vulnerabilities. To learn more about the NECP, visit: https://www.cisa.gov/necp.

Priority Telecommunications Services

CISA provides a suite of communications services that enable public health and safety, national security, and emergency preparedness personnel to communicate with priority when networks are degraded or congested.

Government Emergency Telecommunications Service (GETS) provides emergency access and priority processing over wireline commercial telephone networks at no cost.

Wireless Priority Service (WPS) provides emergency access and priority processing over wireline commercial telephone networks at no cost.

Telecommunications Service Priority (TSP) Program is a Federal Communications Commission program, managed by CISA, which mandates that service providers prioritize the installation (provisioning) and restoration of critical voice and data circuits to facilities that support public health and safety, national security, and emergency preparedness.

Utilizing these services can improve continuity of communications and facilitate mission accomplishment. To register and learn more about Priority Telecommunications Services, visit: https://www.cisa.gov/about-pts.

5.2. Public Messaging

Some cyber incidents require notification of the general public. Given the sensitive nature of cyber incidents, it is important to establish clear procedures for public messaging before an incident occurs. Communication with the public requires awareness of what constitutes sensitive information and includes measures to ensure that sensitive information is protected. If available, a jurisdiction's Public Information Officers may provide assistance with developing and delivering important messages to their communities.

Sensitive Information[15]

Sensitive information can be defined as information that is restricted in some manner based on formal or administrative determination. Examples of such information includes contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and Personally Identifiable Information (PII).

Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Access restrictions may include NDAs. Information flow techniques and security attributes may be used to provide automated assistance to users that make sharing and collaboration decisions.

Not all cyber incidents are publicly reportable. Some may be deemed too sensitive for broader awareness. As such, public messaging protocols for cyber incidents should include steps to determine whether the incident may be publicly reported. For incidents that are reported publicly, ensure that notification regarding resolution of the incident is also distributed.

For those incidents that may be publicly reported, procedures should ensure that only necessary and appropriate information is included in messaging. Measures to ensure appropriate messaging to the public include:

[15] NIST, 2020, *Security and Privacy Controls for Information Systems and Organizations*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Table 1. Appropriate Public Messaging Considerations

DO	DON'T
▪ Determine whether law enforcement entities are more appropriate to develop and deliver messaging; ▪ Use clear and concise language; ▪ Identify any direct or indirect impacts to the safety and security of individuals; ▪ Focus on impacts to service availability; ▪ Emphasize actions that may be taken by the individual to lessen direct impacts; ▪ Emphasize actions that may be taken by the individual immediately to lessen cascading impacts from the initial incident; ▪ Encourage preparedness behaviors that build resilience for future incidents; and ▪ Distribute communications to those within the scope of service disruption	▪ Attribute the incident to any actors until definitive determination by a qualified incident response provider and coordination with federal government partners; ▪ Share specifics related to the location of facilities and assets that are impacted; ▪ Share specifics related to the nature and extent of damage to infrastructure assets; ▪ Identify any ongoing vulnerabilities that may be exploited by opportunistic attackers; ▪ Reference any specific data that have been breached before proper notifications have been made; and ▪ Share any Personally Identifiable Information (PII) or proprietary information

Sample Questions to Consider – Communications Service Loss or Disruption

It is crucial that jurisdictions' continuity assessments and plans include cyber considerations and utilize priority communications during times of degraded communications.

- Are all incident responders and decision makers enrolled in Priority Services, including GETS and WPS? Do they make regular test or training calls and incorporate Priority Services into their training and exercise programs?
- How will requests for TSP restoration be coordinated for any damaged communications services?
- Is the critical infrastructure subscribed to TSP?

Designed to assist public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, the **Communications and Cyber Resiliency Toolkit** is an interactive graphic provided by CISA designed to assist in identifying ways to improve resiliency and develop plans for mitigating the effects of potential resiliency threats. To learn more, visit: https://www.cisa.gov/communications-resiliency.

6. Conclusion

Emergency managers play a central role in preparing jurisdictions for cyber incidents. By coordinating the efforts of planning team members, engaging with stakeholders, and ensuring effective communication, emergency managers develop an understanding of the cyber risks experienced by their jurisdictions and their potential impacts. This understanding and coordination allows for the development and ongoing validation of cyber incident plans, which increases the community's preparedness and overall resilience. Key aspects of cyber incident preparedness include:

- Understanding the types of cyber incidents likely to occur;
- Engaging service owners and operators;
- Identifying critical services and related dependencies;
- Prioritizing and planning for service and system disruptions;
- Clearly identifying roles and responsibilities; and
- Providing integrated communication and public messaging.

This guide aids SLTT emergency management personnel to collaboratively prepare for a cyber incident and support the development of a cyber incident response plan or annex. Appendix A provides details for developing a jurisdiction's cyber plan or supporting annex for an existing emergency operations plan. Appendix C shares additional resources on cyber policy, training, exercise, and funding options. Leveraged together, the information and resources in this guide empower emergency managers to address a persistent and complex hazard to ensure safe and resilient communities.

Appendix A: Developing a Plan

When preparing for cyber incidents, careful planning and collaboration are necessary to ensure a holistic and effective response. Using the six-step planning process detailed in CPG 101: Developing and Maintaining Emergency Operations Plans and shown in Figure 4, the planning team may develop a comprehensive and realistic plan or annex with purposeful involvement from all key stakeholders.

Figure 3. CPG 101 Emergency Operations Six-Step Planning Process

Step 1: Form a Collaborative Planning Team

The most realistic and complete plans result from a diverse planning team that includes representatives from across the whole community. Prior to identifying members of the broader collaborative planning team, it is necessary to identify the core planning team that will be responsible for leading coordination efforts. As CPG 101 suggests, the core planning team is composed of any key partners that are, "likely to be involved in most, if not all, responses." Given the highly technical nature of cyber incident response, it is also important to include key cyber stakeholders on the core planning team.

The wide-reaching threat and impact of a cyber incident necessitate collaboration among many stakeholders in the planning process, to include emergency management, cyber professionals, legal advisors, law enforcement, private industry, and others. However, due to the technical challenges and elements posed by any cyber incident, an essential person to include on the core planning team is the senior information security officer. This could be the senior IT director, chief information officer (CIO), chief information security officer (CISO), chief technology officer (CTO), or designee. If an organization does not have someone with one of these titles, they may seek engagement from the applicable information security officer at the next highest jurisdictional level (e.g., local level, state level).

Once the appropriate information security officer is identified, the emergency manager may work with this individual to identify other members of the core planning team. It is beneficial to include members of the community that have a current understanding of the jurisdiction's continuity plans, cyber infrastructure and cyber security capabilities, as well as any critical connections, roles or features that otherwise would have been unknown. Table 1 below provides a list of individuals/organizations that may be beneficial to include on the core planning team.

Table 2 Potential Stakeholders for the Core Planning Team - Cyber

Individuals/Organizations	Expertise brought to Core Planning Team - Cyber
Emergency Manager or designee	▪ Experience coordinating multiple organizations with varying capabilities and areas of specialized knowledge ▪ Knowledge about all-hazards planning techniques ▪ Knowledge about existing mitigation, emergency, continuity, and recovery plans ▪ Knowledge of emergency communication and response systems that may require cyber systems ▪ Incident management experience and capabilities
Senior IT Director, Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Technology Officer (CTO), or designee[16]	▪ Knowledge of cyber incident response ▪ Specialized personnel and support ▪ Knowledge of key cyber systems within jurisdiction (e.g., water treatment, traffic systems, energy connections, hospital systems, backups)
Senior Official (elected or appointed) or designee	▪ Government intent and priorities by identifying planning goals and essential tasks ▪ Authority to commit the jurisdiction's resources ▪ Knowledge of government resources
Police Chief or designee	▪ Knowledge about local laws and ordinances and specialized response requirements ▪ Knowledge about fusion centers and intelligence and security strategies for the jurisdiction ▪ Knowledge of key law enforcement requiring cyber systems (e.g., dispatch, records, emergency notifications)
Emergency Medical Services Director or designee	▪ Knowledge about emergency medical treatment requirements for a variety of situations ▪ Knowledge of key medical resources that require cyber systems (e.g., dispatch, dispensing)

[16] This is an essential member of the core planning team. If the organization does not have someone with one of these titles, the emergency manager or senior official would seek engagement from the applicable information security officer at the next highest jurisdictional level (e.g., county level, state level).

Individuals/Organizations	Expertise brought to Core Planning Team - Cyber
Fire Chief or designee	▪ Knowledge about the jurisdiction's fire-related risks ▪ Knowledge of key fire resources that require cyber systems (e.g., dispatch)
Public Works Director or designee	▪ Knowledge about the jurisdiction's road and utility infrastructure and the cyber-based systems in use (e.g., traffic systems, road signage)
Public Health Officer or designee	▪ Understanding of the unique medical needs of the community
General counsel or legal advisor	▪ Knowledge of applicable data privacy laws and other legal requirements

Given the potential reach and scope of a disruptive cyber incident, it is important to include additional community stakeholders in the planning process through the broader collaborative planning team, including those associated with community lifelines and other critical services that rely on cyber systems. Examples of key stakeholders that may be beneficial to include on the broader collaborative planning team are presented in Table 2.

Table 3. Potential Stakeholders for the Collaborative Planning Team - Cyber

Individuals/Organizations	Expertise brought to Collaborative Planning Team - Cyber
Utility representatives or designee	▪ Knowledge about utility infrastructure and possible cyber interdependencies (e.g., connections to and from gas, electric, and water interconnections)
Hazardous Materials Coordinator or designee	▪ Knowledge about hazardous materials that are produced, stored, or transported in or through the community, and the cyber-based systems in use (e.g., facility controls, machinery)
Transportation Director or designee	▪ Knowledge about the jurisdiction's road infrastructure and transportation resources and the cyber-based systems in use (e.g., traffic systems, camera operations)
School Superintendent or designee	▪ Knowledge about the hazards that directly affect schools and the cyber-based systems in use (e.g., administrative systems, communication software, enrollment information)

Individuals/Organizations	Expertise brought to Collaborative Planning Team - Cyber
Local federal response partners or designee, to include Protective Security Advisors/Cyber Security Advisors and others[17]	▪ Knowledge about specialized personnel and equipment resources that could be used in an emergency (e.g., CIRT teams) ▪ Knowledge about potential threats to or hazards at federal facilities ▪ Knowledge of regional interconnections and partnerships that may be able to assist with a cyber incident ▪ Understanding of broader level threat landscape that may be required for overall containment of cyber threat
Nongovernmental organizations and other private, not-for-profit, faith-based, and community organizations or designee	▪ Knowledge about community resources and needs ▪ Understanding of community and its communication needs (e.g., case management systems)
Local business and industry senior IT representatives or designee	▪ Knowledge of their IT infrastructure and their dependencies (e.g., cash system, security system, communications)

Step 2: Understand the Situation

In this step, the planning team develops an understanding of how potential incidents may occur in and impact their community. Information in the Types of Cyber Incidents section of this guide provides a starting point for understanding the common types of cyber incidents and how they could impact the community. The Assessing Cyber Risks to Inform Prioritization and Planning section provides guidance and considerations for identifying potential consequences and impacts from cyber incidents and restoration priorities.

The planning team may benefit from developing a few scenarios to drive their planning efforts. Not every cyber incident will require a broad community response, or even a response outside the affected entity. Developing and exploring different scenarios helps the planning team understand the potential risks to be addressed in the response plan or annex and to examine the dependencies of assets and services. Exercises may also be used after the plan is developed to identify potential gaps and highlight where additional training and coordination is needed.

Prior to developing a cyber incident plan or annex, or integrating cyber incidents into a jurisdiction's emergency operations plan (EOP), the planning team should fully understand their EOP and any

[17] PSAs are trained critical infrastructure protection and vulnerability mitigation subject matter experts who facilitate local field activities in coordination with other Department of Homeland Security offices. They also advise and assist state, local and private sector officials and critical infrastructure facility owners and operators. For more information visit: https://www.cisa.gov/protective-security-advisors.

existing supporting plans and annexes, such as communications and energy. Annexes supplement and are consistent with the EOP and do not duplicate or conflict with it. A jurisdiction's EOP base plan or supporting plans will address many responsibilities and actions taken when implementing cyber incident response, as these actions are frequently required regardless of the specific threat or hazard. A cyber annex therefore addresses the unique characteristics and requirements not already covered in the EOP base plan or other annexes.

Step 3: Determine Goals and Objectives

In this step, the planning team works together to determine operational priorities and then sets goals and objectives for cyber incident response. Operational priorities specify what the responding organizations intends to accomplish and the desired end-state for the cyber incident response. Using the scenarios and risk analysis results from Step 2, the planning team engages the senior official (e.g., tribal leader[s], mayor, county judge, commissioner[s]) to explore how the incident and impacts may evolve within the jurisdiction and what defines a successful outcome. The resulting discussion explores the requirements necessary to achieve the desired end-state, which will help determine actions and resources needed for the incident response. Senior officials may identify the desired end-state and operational priorities for cyber incident response operations or affirm those proposed by the planning team.

The actual situation when an incident occurs will determine the incident objectives. The goals and objectives established in the EOP are based on planning assumptions and provide a starting place for incident response planning.

Once operational priorities for the EOP or annex are set, the planning team collectively determines goals and objectives for cyber incident response. The goals and objectives should be realistic and based on the current state of cyber maturity in the jurisdiction. When crafting goals and objectives, the planning team considers the minimum capabilities needed to provide essential services and understands that priorities may change during the course of the incident.

Possible Goals for a Cyber Incident Response Plan May Include:

- Ensure continuous operations of community lifelines and critical services.
- Disseminate timely information to the community regarding impacted services, restoration expectations, and available support.
- Efficiently exchange information with service owners/operators to enable rapid response and recovery efforts.
- Mitigate additional cascading impacts by isolating the impacted system(s), if possible.
- Identify how the system was compromised and make the immediate changes to ensure vulnerabilities cannot continue to be exploited while containment and recovery efforts are ongoing.

Step 4: Develop the Plan

Based on the results of Steps 2 and 3, the planning team may begin developing their plan, to include generating, comparing, and selecting possible courses of action to achieve the identified goals and objectives and identifying resources. Planners may refer to CPG 101 for writing and reviewing checklists, as well as format considerations.

The cyber experts on the planning team play an essential role in developing and evaluating courses of action, as they may provide insight into the likely actions, impacts, and decision points in a cyber incident. When developing courses of action, the planning team may follow the process described in CPG 101. During this decision process, the planning team considers:

- The roles and responsibilities each party may play throughout a cyber incident. For example, an emergency manager may provide support in an emergency caused by a cyber incident or may be responsible for leading the response if the cyber incident resulted in physical damages to water treatment or fuel supply facilities;
- A timeline of when expected response parties would be available;
- Specific types of cyber incidents that would require special notifications or cause concern that may require notification to legal authorities, neighboring jurisdictions, state, or federal governments; and
- When to ask for additional specialized assistance and determine what options are available.

When developing courses of action, the planning team considers any applicable legal requirements or procedures. Cyber incidents, such as those involving data breaches, may necessitate compliance with specific legal reporting requirements. Laws might specify when and how to disclose privacy or identify risks, such as the breach of private personal information. For example, if a data breach affects financial information such as payment (credit/debit) cards, the organization may need to notify consumer reporting agencies and the payment card issuers and processing companies.

Considering an Effects-Based Approach

When planning for a cyber incident, it can be difficult to predict the impact of cascading failures across infrastructures because unknown and unintended consequences are probable, given the ever-increasing complexity and connectedness of infrastructure. As such, jurisdictions may benefit from considering the potential effects of an incident when developing and selecting courses of action. These effects often fall into at least one of the following categories: loss of power, loss of internet, loss of local networks, loss of voice communications, loss of local IT equipment, loss of access to data, and loss of key IT personnel.

Effects-based planning can serve as a vehicle to bring together disparate groups to focus on how to strengthen response posture and improve resiliency.

After selecting courses of action, the planning team determines what resources are necessary to carry out the associated activities and identifies resource gaps so that they may work with partners to preemptively address those gaps. The planning team may use capability estimates to describe the jurisdiction's ability to perform a course of action. When developing capability estimates for cyber incident response planning, the planning team may want to consider:

- Cyber Incident Response Teams (CIRT);
- State/federal partners;
- Mutual aid assistance;
- Third-party cyber advisors, which may be private sector partners;
- Computer equipment (e.g., laptops, monitors, networking);
- Industrial control system hardware (e.g., human machine interfaces);
- Communications (e.g., telephone, network); and,
- Computer storage (e.g., hard drives).

Establishing a Cyber Disruption Team (CDT)

Jurisdictions may want to consider establishing a CDT in their plan. A CDT is a specialized consultative group comprised of representatives and subject matter experts from emergency management, IT, law enforcement, critical infrastructure, and other relevant domains. The CDT is a key resource for understanding:

- the nature and potential durations of cyber disruptions;
- the effects of cyber disruptions on critical life-safety, critical cyber assets, and other key response activities; and
- the potential resource needs of IT personnel and agencies to maintain, protect, and re-establish operations.

During cyber disruptions of any nature, the CDT will integrate into the Incident Command System (ICS) structure of the overall incident response. Utilizing the CDT framework incorporates the added benefit of integrating emergency management principles and procedures for IT personnel and other disciplines.

Depending on the impacts of an incident, emergency managers may need to activate other plans or annexes (e.g., power outage, distribution management). Activation of other plans may require incorporation of additional partners into incident support and consequence management functions. Establishing a unified coordination structure aims to effectively integrate partners with leadership roles into a complex cyber incident that includes extensive cascading impacts.

During this step, the planning team also determines how to assess the status and operational readiness of the previously identified essential services and cyber assets and factors that information into plan development. This will help when responding to cyber incidents by providing emergency managers with information about what and how services are affected, what services are not affected, and what services might be affected later.

Step 5: Prepare and Review the Plan

This step involves translating the findings of Steps 3 and 4 into a cyber incident response plan or annex, reviewing it to ensure that it meets applicable regulatory requirements and jurisdictional standards, verifying that it is useful in practice, and obtaining approval on the plan by the appropriate authorized body. During this step, jurisdictions may update key stakeholders and receive buy-in from partners. Planners may follow the best practices for plan development outlined in CPG 101 to ensure the plan is readily understood by all audiences regardless of their technical expertise.

To ensure the plan meets regulatory requirements and standards, the planning team may engage external partners (e.g., the next level of government, regional or national cyber experts) to perform a review of the document. To evaluate the effectiveness of the plan, the planning team may consider the five criteria outlined in CPG 101: adequacy, feasibility, acceptability, completeness, and compliance.

Questions to Consider When Reviewing a Cyber Incident Plan or Annex

- Did the planning team include representation from the jurisdiction's technology teams?
- Does the plan outline the roles and responsibilities of the key stakeholders?
- Does the plan map interdependencies between critical cyber systems or services?
- Does the plan include an emergency contact list for each of the critical cyber services?
- Does the plan identify potential consequences of service disruptions?
- Does the plan outline minimal service levels needed to maintain continuity of operations?
- Does the plan clearly identify available cyber response resources (e.g., personnel, administration and finance, operational organizations, logistics, communications, equipment, facilities)?
- Does the plan specify how to notify emergency management of an event with potentially cascading impacts to other areas?
- Does the plan identify when to escalate emergency response and who is responsible for making that decision?
- Does the plan clearly define the beginning and end of cyber incident response operations?
- Does the plan clearly define who is the lead, who are the support roles, and how to divide and address necessary tasks during cyber incident response?
- Does the plan include provisions for engaging private sector organizations in the management of cyber incident response either as resources or as members of the unified coordination group?
- Does the plan account for updates in technology since the last revision?

Prior to distributing the approved cyber incident response plan or annex, the planning team would confirm that the document does not contain any sensitive information that could be leveraged to carry out a cyberattack. Sensitive information may need to be redacted, or the plan's distribution limited to a smaller, specific audience as described earlier in the Communications Considerations section.

Step 6: Implement and Maintain the Plan

This step focuses on ensuring key stakeholders are familiar with the roles and processes described in the plan or annex, through training and exercises, and that the plan or annex is regularly updated to reflect lessons learned and best practices.

Training on the cyber incident response plan or annex is crucial to preparing the response team for timely communication and coordination activities. Routine training also helps ensure new staff are aware of their roles and responsibilities. It may be beneficial for trainings to address:

- Foundational cyber topics (e.g., common causes of cyber incidents, key terms);
- Basic topics in emergency management (e.g., planning, situational awareness, Incident Command System) for other key personnel (e.g., IT staff, CISO);
- Use of specific, essential response tools (e.g., decision support matrices, escalation criteria);
- Complex or nuanced aspects of response (e.g., notification, escalation, legal reporting requirements); and,
- Plan specific training (e.g., communication relay, role/function assignments).

Like other emergency plans and annexes, cyber incident response plans are exercised regularly. Use of Homeland Security Exercise and Evaluation Program (HSEEP) guidance can maximize the effectiveness of exercise development. Once exercise scope, objectives, and capabilities are identified, exercise planners may develop scenarios for their exercise. It is important for the exercise planning team to include cyber experts in both the exercise planning and after-action processes. These cyber experts help to ensure the cyber aspects of the exercise are realistic while understanding and interpreting the more nuanced aspects of a cyber incident so improvement actions are documented accurately. Jurisdictions may select to integrate cyber considerations into their broader exercise program, to include the Integrated Preparedness Planning Workshop and resultant multi-year Integrated Preparedness Plan recommended in the Homeland Security Exercise and Evaluation Program.

Michigan Statewide Cyber Disruption Exercise

As part of an annual scenario-based exercise series on cyber disruptions, Michigan conducted a functional exercise in 2021 to test the state's ability to respond to a simultaneous cyber-attack on multiple local governments and K-12 schools. The scenario was based on threat models, indicators of compromise, and actual events in Michigan and other states.

The exercise goals provided a scenario that grew in complexity and allowed teams to exercise response, interagency coordination, and communication capabilities. The exercise itself involved players from planning team organizations, local governments, and school districts.

Exercise planning included multiple organizations providing complimentary and overlapping skillsets, but with different capabilities and reporting structures. Preparation for the exercise included coordination among the major players to ensure mutual understanding and documentation of capabilities, command structures, and activation procedures.

Major planning organizations and key functions related to the exercise included:

- Michigan State Police Emergency Management and Homeland Security Division (MSP/EMHSD), responsible for emergency operations coordination and the State Emergency Operations Center;
- MSP Michigan Cyber Command Center (MC3), responsible for cyber emergency response coordination during critical incidents in the state;
- Michigan Department of Technology, Management, and Budget (DTMB) resources, including the Michigan Cyber Civilian Corps, trained technical experts who volunteer to local incidents when requested; and Michigan Cyber Partners, a collaboration of various state and local public entities who help local entities prepare for cyber incidents;
- Michigan National Guard, provides advanced cyber defense capabilities available to support state government and civilian industry; and
- Federal agencies including CISA and the FBI who work closely with state and local partners and provide national context to local incidents.

Highlights and lessons learned from the exercise:

- The planning process for the exercise allowed for state cyber response plans to be updated simultaneously;
- Experiences were applied in 2022 when using the Michigan Cyber Disruption Response Plan to aid in real-world interagency coordination and communication regarding the Russian/Ukrainian war and cybersecurity related threats to the state.
- The cycle of planning, training, and exercising together was essential to gain knowledge, understand organizational capabilities, close capability gaps, and build trusted relationships.

Exercise Resources

- The Homeland Security Exercise and Evaluation Program (HSEEP): Provides a set of guiding principles for exercise and evaluation programs, including a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. Utilizing HSEEP helps to ensure a coordinated and comprehensive approach to planning, training, and strengthening capabilities ahead of a cyber incident.
- National Exercise Program (NEP) is a two-year cycle of exercises across the nation that examines and validates capabilities in all preparedness mission areas. SLTT jurisdictions are eligible to submit requests for exercise support and participate in the NEP.
- HSEEP After-Action Report Template: Provides a flexible template for after action report development.
- CISA Tabletop Exercise Packages (CTEPs): A comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Packages include cybersecurity Situation Manuals (SITMANs) covering topics such as industrial control systems (ICS), ransomware, insider threats, phishing, and elections-related cyber threat vectors.

Appendix B: Cyber Incident Identification and Closing Processes

The planning team works together to establish a process for monitoring, identifying, and declaring a cyber incident. The planning team identifies benchmarks or triggers that clearly indicate when the cyber incident plan or annex is activated. As a starting point for this effort, it may be helpful for the planning team to review the Cyber Incident Severity Schema in the National Cyber Incident Response Plan (NCIRP), which serves as a way to describe the severity or impact of a cyber incident.

For cyber-driven events, the first partners to notified often vary based on the incident and jurisdiction. This means that building strong relationships and understandings of cascading impacts from cyber incidents may enhance the capacity to make joint and informed decisions. Establishing relationships and reviewing cyber incident response protocols with these types of partners helps emergency managers gain an understanding of the types of situations they would be asked to assist or lead for a cyber-driven event. To report a cyber incident to CISA visit the Incident Reporting System.[18]

The planning team may also choose to establish benchmarks or triggers that signal the end of cyber incident response operations and a return to regular activities. For instance, a cyber incident response may end once the root cause of the incident has been identified and remediated or the situation stabilized. Cyber incidents often escalate and de-escalate differently than natural hazards. For example, while hurricanes often come with significant pre-warning and progress in severity, cyber incidents may have unexpected and immediate severe impacts. Similarly, other disasters may include a long-term recovery process that lasts months or years. Although cyber professionals may consider a cyber incident fully recovered once the compromised system is restored to functionality, the physical and cascading impacts of a cyber incident may require a longer recovery process. Open and regular communication among staff is key to understanding how similar terms are used in different organizations and for establishing clear expectations.

The end of a cyber incident may be hard to define, as it may blend into traditional recovery activities. Officially closing a cyber incident indicates that the situation has stabilized and allows for regular activities.

[18] https://www.cisa.gov/forms/report.

Cybersecurity Incident & Vulnerability Response Playbooks

CISA developed two playbooks to strengthen cybersecurity response practices and operational procedures for the federal government, public, and private sector entities. Building on insights from previous incidents and incorporating industry best practices, the playbooks contain checklists for incident response, incident response preparation, and vulnerability response that any organization can adapt to track necessary activities to completion.

- The Incident Response Playbook applies to incidents that involve confirmed malicious cyber activity and for which a major incident has been declared or not yet been reasonably ruled out.
- The Vulnerability Response Playbook applies to any vulnerability used by adversaries to gain unauthorized entry into computing resources. This playbook builds on CISA's Binding Operational Directive 22-01 and standardizes the high-level process that is followed when responding to vulnerabilities that pose significant risk across the federal government, and private, and public sectors.

To view the playbooks visit: Federal Government Cybersecurity Incident and Vulnerability Response Playbooks (cisa.gov).

Appendix C. Additional Resources

Cyber Incident Management Guidance, References, and Training

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

- Emergency Directives and Binding Operational Directives: Provide actionable guidance in response to specific cybersecurity threats. Although Binding Operational Directives (BODs) and Emergency Directives (EDs) strictly apply to and require action from Federal Civilian Executive Branch agencies, the threats they address often extend to every sector. Therefore, CISA recommends all stakeholders review and adopt BOD and ED guidance.
- Binding Operational Directive 22-01: Establishes a CISA-managed catalog of known exploited vulnerabilities that carry significant risk to the federal enterprise and establishes requirements for agencies to remediate any such vulnerabilities.
- CISA Vulnerability Scanning: Provides automated vulnerability scans and delivers a weekly report, which helps secure internet-facing systems from weak configurations and known vulnerabilities.
- Cyber Essential Element -- Your Crisis Response: Provides tips focused on limiting damage and quickening restoration of normal operations.
- Cyber Essentials Starter Kit: Provides guidance for leaders of small businesses and small and local government agencies to help them start implementing organizational cybersecurity practices.
- Cybersecurity Glossary: A glossary of common cybersecurity words and phrases.
- Cyber Resilience Review (CRR): A no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by the Department of Homeland Security (DHS) cybersecurity professionals. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.
- Cyber Incident Resource Guide for Governors: Information for governors and their staff on how to request federal support during or following a cyber incident.
- Cyber Incident Response Resources: Provides an overview of CISA's role in cyber incident response and includes supporting resources.

- Cyber Incident Response Training: No-cost cybersecurity incident response training for government employees and contractors across federal and SLTT government, and educational and critical infrastructure partners.
- Cybersecurity Performance Goals: Provide baseline IT and OT security practices that can improve resilience against, and meaningfully reduce the likelihood and impact of, known cyber risks and common TTPs.
- Cyber Security Evaluation Tool (CSET): Provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. CSET includes the Cybersecurity Performance Goals Assessment, which organizations can use to evaluate their cybersecurity posture and drive investments towards meaningfully reducing the likelihood and impact of known risks and adversary techniques.
- Emergency Services Sector Cybersecurity Framework Implementation Guidance: Provides foundational guidance for how emergency services sector organizations may enhance their cybersecurity using the NIST Cybersecurity Framework.
- Emergency Services Sector Cybersecurity Initiative: Provides resources to help those in the emergency services sector better understand and manage cyber risks.
- Federal Government Cybersecurity Incident and Vulnerability Response Playbooks: Two playbooks developed by CISA to strengthen cybersecurity practices and operational procedures for the federal government, and public and private sector entities. The playbooks contain checklists for incident response, incident response preparation, and vulnerability response.
- Free Cybersecurity Services and Tools: Identifies free cybersecurity tools and services to help organizations further advance their security capabilities.
- Resources for State, Local, Tribal and Territorial (SLTT) Governments: Presents key resources for SLTT governments pertaining to cybersecurity, including best practices, case studies, and an SLTT Toolkit.
- State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC) Cyber Resource Compendium: Identifies some of the major references that may help build or strengthen an organization's cybersecurity program.
- Tabletop Exercise Packages (CTEPs): A comprehensive set of resources designed to assist stakeholders in conducting their own exercises. The packages include cybersecurity situation manuals covering topics such as industrial control systems, ransomware, insider threats, phishing, and elections-related cyber threats.

FEDERAL EMERGENCY MANAGEMENT AGENCY

- Building Private-Public Partnership Guide: Provides best practices for jurisdictions to establish and maintain a private-public partnership, which is essential to successful cyber incident response.
- Continuity Resources and Technical Assistance: Information and tools on continuity of operations plans, assessments, and resources.
- Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining Emergency Operations Plans: Details the six-step planning process for developing emergency operations plans and hazard specific annexes.
- Comprehensive Preparedness Guide (CPG) 201: Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Guide (SPG): Provides guidance for communities on conducting THIRA and SPR assessments and evaluating levels of preparedness.
- Homeland Security Exercise and Evaluation Program (HSEEP): Provides a set of guiding principles for exercise and evaluation programs, including a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.
- HSEEP After-Action Report Template: Provides a flexible template for after action report development.
- National Exercise Program (NEP): A two-year cycle of exercises across the nation that examines and validates capabilities in all preparedness mission areas. SLTT jurisdictions are eligible to submit requests for exercise support and participate in the NEP.
- National Incident Management System: Guides all levels of government, nongovernmental organizations, and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents by providing the whole community with shared vocabulary, systems, and processes.
- Preparedness Grants Manual: Describes regulations, policies, and procedures for managing preparedness grants with guidance specific to each grant. Includes information on the Homeland Security Grant Program.
- Threat and Hazard Identification and Risk Assessment (THIRA): Provides guidance for assessing the risk of all threats and hazards.

NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

- Computer Security Incident Handling Guide: Assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively.

- Cybersecurity Framework: Provides strategic guidance to help build and execute a cybersecurity program. Helps organizations assess cyber risks and set plans for improving or maintaining their security posture.
- Guide for Conducting Risk Assessments: Provides guidance for conducting risk assessments of federal information systems and organizations.
- Guide for Cybersecurity Event Recovery: Provides guidance to help organizations plan and prepare for recovery from a cyber event and integrate the processes and procedures into their enterprise risk management plans.
- Security and Privacy Controls for Information Systems and Organizations: Provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, and other organizations from a diverse set of threats and risks.

OTHER RESOURCES

- Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government: Explains when, what, and how to report a cyber incident to the federal government.
- Data Breach Response Guide: Provided by the Federal Trade Commission and provides general guidance for an organization on how to manage a data breach.
- National Cyber Incident Response Plan (NCIRP): Maintained by the Department of Homeland Security, the NCIRP is a national approach to dealing with cyber incidents. It addresses the important role that the private sector, state and local governments, and multiple federal agencies play in responding to incidents and how the actions of all fit together for an integrated response.

Direct Resources and Partnerships

MULTI-STATE INFORMATION SHARING & ANALYSIS CENTER (MS-ISAC)

In addition to working to help improve the cybersecurity posture of SLTT governments, MS-ISAC operates a cybersecurity operations center 24 hours a day, 7 days a week to provide real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.

The MS-ISAC Cyber Incident Response Team (CIRT) provides SLTT governments with malware analysis, computer and network forensics, code analysis/mitigation, and incident response. External vulnerability assessments are also available after an incident. This service helps victims of cyber incidents to check if their remediation efforts have been effective. For more information, visit: https://www.cisecurity.org/ms-isac/.

SLTT government representatives who believe they are experiencing a cybersecurity event may report it to: https://www.cisecurity.org/isac/report-an-incident.

CYBER SECURITY ADVISORS (CSA)

CSAs are regionally located DHS personnel who direct coordination, outreach and regional support to protect cyber components essential to the sustainability, preparedness and protection of the Nation's critical infrastructure and SLTT governments. CSAs offer immediate and sustained assistance to prepare and protect SLTT and private entities. CSAs bolster the cybersecurity preparedness, risk mitigation, and incident response capabilities of these entities and bring them into closer coordination with the federal government. CSAs represent a front-line approach and promote resilience of key cyber infrastructures throughout the U.S. and its territories. For more information about CSAs, please email cyberadvisor@hq.dhs.gov.

EMERGENCY COMMUNICATIONS COORDINATORS (ECC)

ECCs are subject matter experts located across the country who build trusted relationships, enhance collaboration, and stimulate the sharing of best practices and information between all levels of government, critical infrastructure owners and operators, and key non-government organizations. ECCs seek to build partnerships between federal, state, local, tribal, and territorial government stakeholders as well as the private sector. These partnerships result in a united effort to improve the Nation's operable and interoperable emergency communications. For more information on the Emergency Communications Coordination Program, please visit: https://www.cisa.gov/emergency-communications-coordination-program.

PROTECTIVE SECURITY ADVISOR (PSA)

PSAs are trained critical infrastructure protection and vulnerability mitigation subject matter experts. Operating under CISA's Integrated Operations Division, PSAs facilitate local field activities in coordination with other DHS offices while assisting state, local, private sector, and critical infrastructure officials, owners and operators. The PSA program focuses on physical site security and resiliency assessments, planning and engagement, incident management assistance, and vulnerability and consequence information sharing. For more information about PSAs, visit: https://www.cisa.gov/security-advisors.

PUBLIC INFRASTRUCTURE SECURITY CYBER EDUCATION SYSTEM (PISCES)

PISCES is a non-profit organization that, in partnership with DHS CISA and the Pacific Northwest National Laboratory, partners with the private sector, colleges and universities, and local governments to provide no-cost cybersecurity event monitoring to small public sector organizations. Students leverage data collected from customer networks to build their skills as cybersecurity analysts, and report confirmed or potential compromises to the customer jurisdiction when identified. For more PISCES information, visit: pisces-intl.org.

Funding Considerations

ROBERT T. STAFFORD DISASTER RELIEF AND EMERGENCY ASSISTANCE ACT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act[19] (Stafford Act) authorizes the President to declare a major disaster or emergency and provide federal assistance to states, territories, local governments, tribal nations, individuals and households and nonprofit organizations to respond and recover from a major disaster. All requests for a declaration by the President are made by the governor or tribal leader of the affected state, territory, or tribal nation. These requests are based on findings that "the disaster is of such severity and magnitude that effective response is beyond the capabilities of the State and the affected local governments, and that Federal assistance is necessary."

Cyber incidents may or may not meet the criteria for declaring a major disaster or emergency. During a cyber incident response, jurisdictions may need additional resources including computer hardware, software, cybersecurity services from vendors, and other support services or personnel. Planning for a potential widespread cyber incident, including the identification of various resource and funding sources, is critical for jurisdictions.

HOMELAND SECURITY PREPAREDNESS GRANTS

The Homeland Security Grant Program includes a suite of risk-based grants to assist state, local, tribal, and territorial efforts in preventing, protecting against, mitigating, responding to, and recovering from acts of terrorism and other threats. These grants provide grantees with the resources required for implementation of the National Preparedness System and working toward the National Preparedness Goal (NPG) of a secure and resilient nation.

In addition to other items allowed under the grants, certain cybersecurity planning, risk reduction activities, and hardware and operating system software designated for use in an integrated system, may be allowable under specific grant programs. Such systems include detection, communication, cybersecurity, and geospatial information systems.

For more information on Homeland Security Grants, visit: https://www.fema.gov/grants/preparedness/homeland-security#programs.

CYBERSECURITY GRANT PROGRAMS

The passage of the Infrastructure Investment and Jobs Act of 2021 established the State and Local Cybersecurity Grant Program (SLCGP) and Tribal Cybersecurity Grant Program (TCGP). Implemented by CISA and FEMA, CISA serves as a programmatic subject matter expert for the programs, while FEMA provides grant administration and oversight for appropriated funds. For the SLCGP, state and territorial governments are responsible for cybersecurity planning and project development as well

[19] Pub. L. No. 93-288, as amended, 42 U.S.C. 5121 et seq.

as pass-through responsibilities to include distributing awarded funds to local governments to address cybersecurity risks and threats to information systems owned or operated by or on behalf of state, local, tribal, and territorial governments. For the TCGP, the tribal governments are recipients responsible for cybersecurity planning and project development, but no required pass-through of funding to other entities.

The overarching goal of the programs is to assist state, local, tribal, and territorial governments in managing and reducing systemic cyber risks. To accomplish this, CISA established four separate, but interrelated objectives:

- **Governance and Planning:** Develop and establish appropriate governance structures, as well as plans, to improve capabilities to respond to cybersecurity incidents and ensure the continuity of operations.
- **Assessment and Evaluation:** Identify areas for improvement in SLTT cybersecurity posture based on continuous testing, evaluation, and structured assessments.
- **Mitigation:** Implement security protections commensurate with risk through best practices.
- **Workforce Development:** Ensure organizational personnel are appropriately trained in cybersecurity, commensurate with their responsibilities as suggested in the National Initiative for Cybersecurity Education.[20]

For more information on the State and Local Cybersecurity Grant Program and the Tribal Cybersecurity Grant Program, email FEMA-SLCGP@fema.dhs.gov or FEMA-TCGP@fema.dhs.gov or visit https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program or https://www.cisa.gov/cybergrants.

CYBER RESPONSE AND RECOVERY FUND

The passage of the Infrastructure Investment and Jobs Act also included the Cyber Response and Recovery Act (CRRA), which authorizes the Secretary of Homeland Security to declare a significant cyber incident under specific circumstances. The CRRA also establishes the Cyber Response and Recovery Fund (CRRF), which CISA can use following a declaration to coordinate asset response activities, provide response and recovery support for the specific significant incident (including through asset response activities and technical assistance), and, as the CISA Director determines appropriate, award grants or cooperative agreements to help entities respond to or recover from the specific significant incident. Once the grant program is established, it will be implemented by CISA. After the program is established and implemented, CISA will provide more information to the public on the circumstances under which a grant can be awarded.

[20] https://www.nist.gov/itl/applied-cybersecurity/nice

Appendix D: Glossary

- **Asset**: Items of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation).
- **Attack**: An attempt to gain unauthorized access to system services, resources or information, or an attempt to compromise system integrity.
- **Confidentiality**: A property that information is not disclosed to users, processes, or devices unless they have been authorized to access the information.
- **Continuity Plan:** A documented plan that details how an individual organization will ensure it can continue to perform its essential functions during a wide range of incidents that impact normal operations.
- **Cyber Incident**: An event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.
- **Cyber Infrastructure**: Electronic information, communications systems, services, and the information contained therein.
- **Cybersecurity**: The activity or process, ability or capability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
- **Data Breach**: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.
- **Denial-of-Service (DoS)**: An attack that prevents or impairs the authorized use of information system resources or services.
- **Disruption**: An event which causes unplanned interruption in operations or functions.
- **Distributed Denial-of-Service (DDoS)**: A denial of service technique that uses numerous systems to perform the attack simultaneously.
- **Downstream Dependencies:** Services provided by a jurisdiction to its residents or other jurisdictions.

- **Exploit**: A technique to breach the security of a network or information system in violation of security policy.

- **Incident Command System (ICS)**: A standardized approach to the command, control, and coordination of on-scene incident management, providing a common hierarchy within which personnel from multiple organizations may be effective. ICS is the combination of procedures, personnel, facilities, equipment, and communications operating within a common organizational structure, designed to aid in the management of on-scene resources during incidents. It is used for all kinds of incidents and is applicable to small, as well as large and complex, incidents, including planned events.

- **Industrial Control System (ICS)**: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution or to control infrastructure assets. It is also known as operational technology.

- **Information Technology (IT)**: Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

- **Insider Threat**: A person or group of persons within an organization who pose a potential risk through violating security policies. One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that enabling them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.

- **Integrity**: The property whereby information, an information system or a component of a system has not been modified or destroyed in an unauthorized manner. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

- **Malware**: Software that compromises the operation of a system by performing an unauthorized function or process. Hardware, firmware, or software that is intentionally included or inserted in a system to perform an unauthorized function or process that has adverse impacts on the confidentiality, integrity, or availability of an information system.

- **Mitigation**: The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences.

- **Network Services**: Firewalls, including relevant hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

- **Operational Technology (OT)**: The hardware and software systems used to operate industrial control devices.
- **Phishing**: A digital form of social engineering to deceive individuals into providing sensitive information, including usernames and passwords.
- **Privacy**: The assurance that the confidentiality of, and access to, certain information about an entity is protected.
- **Recovery**: The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.
- **Resilience**: The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.
- **Service**: A resource or capability provided by an asset that may be used for operational or information functions.
- **Significant Cyber Incident**: A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.
- **Spyware**: Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.
- **System**: A combination of interacting elements organized to achieve one or more stated purposes. Interacting elements in the definition of system include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities. Source: NIST SP 800-160 Vol. 2 Rev. 1.
- **Trojan:** A computer program that appears to be useful by evading security mechanisms, but aims to harm a system or steal information, sometimes through exploiting legitimate authorizations of a system entity invoking the program.
- **Unauthorized Access**: Any access that violates the stated security policy.
- **Upstream Dependencies:** These are products or services provided to a jurisdiction by an external organization that are necessary to support its operations and functions.
- **Worm:** A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Appendix E: Acronyms

BOD	Binding Operational Directive
CDT	Cyber Disruption Team
CIO	Chief Information Officer
CIRT	Cyber Incident Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CPG	Comprehensive Preparedness Guide
CRR	Cyber Resilience Review
CSET	Cyber Security Evaluation Tool
CRRA	Cyber Response and Recovery Act
CRRF	Cyber Response and Recovery Fund
CTO	Chief Technology Officer
DHS	Department of Homeland Security
DOS	Denial of Service
EOP	Emergency Operations Plan
FEMA	Federal Emergency Management Agency
GETS	Government Emergency Telecommunications Service
HSEEP	Homeland Security Exercise and Evaluation Program
ICS	Industrial Control Systems OR Incident Command System
ISAC	Information Sharing & Analysis Center
IT	Information Technology
KEV	Known Exploited Vulnerability

NCIRP	National Cyber Incident Response Plan
NCSR	Nationwide Cybersecurity Review
NDA	Non-Disclosure Agreement
NECP	National Emergency Communications Plan
NIMS	National Incident Management System
NIST	National Institute of Science and Technology
OT	Operational Technology
PACE	Primary, Alternate, Contingency, and Emergency
PII	Personally Identifiable Information
PISCES	Public Infrastructure Security Cyber Education System
PSA	Protective Security Advisor
SLTT	State, Local, Tribal, and Territorial
THIRA	Threat and Hazard Identification and Risk Assessment
TSP	Telecommunications Service Priority
TTP	Tactics, Techniques, and Procedures
UCG	Unified Coordination Group
WPS	Wireless Priority Service