NATIONAL CYBER INCIDENT RESPONSE PLAN

December 2016

Homeland Security

This page intentionally left blank.

Table of Contents

Executive Summary

Networked technologies touch every corner of the globe and every facet of human life. They have driven innovation, nurtured freedoms, and spurred economic prosperity. Even so, the very technologies that enable these benefits offer new opportunities for malicious and unwanted cyber activities. The risks associated with the Nation's dependence on these networked technologies led to the development of Presidential Policy Directive 41 (PPD-41): *United States Cyber Incident Coordination*, which sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities.

PPD-41 recognizes that the frequency of cyber incidents is increasing, and this trend is unlikely to be reversed anytime soon. The most significant of these incidents, those 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, necessitate deliberative planning, coordination, and exercising of response activities, in order to minimize the threat and consequences to the Nation, infrastructure, and way of life.

The National Cyber Incident Response Plan (NCIRP or Plan) was developed according to the direction of PPD-41 and leveraging doctrine from the National Preparedness System to articulate the roles and responsibilities, capabilities, and coordinating structures that support how the Nation responds to and recovers from significant cyber incidents posing risks to critical infrastructure. The NCIRP is not a tactical or operational plan; rather, it serves as the primary strategic framework for stakeholders to understand how federal departments and agencies and other national-level partners provide resources to support response operations. Authored in close coordination with government and private sector partners, the NCIRP expounds upon the concurrent lines of effort, defined by PPD-41, for how the Federal Government will organize its activities to manage the effects of significant cyber incidents. The concurrent lines of effort are threat response, asset response, intelligence support, and the affected entity, which undertakes efforts to manage the effects of the incident on its operations, customers, and workforce. The activities and lead federal agencies for each line of effort within the Cyber Unified Coordination Group are described below.

- The Department of Justice is the lead agency for threat response during a significant cyber incident, acting through the Federal Bureau of Investigations and National Cyber Investigative Joint Task Force. Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.

- The Department of Homeland Security is the lead agency for asset response during a significant cyber incident, acting through the National Cybersecurity and Communications Integration Center. Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery.

- Threat and asset responders will share some responsibilities and activities, which may include communicating with affected entities to understand the nature of the cyber incident; providing guidance to affected entities on available federal resources and capabilities; promptly disseminating through appropriate channels intelligence and information learned in the course of the response; and facilitating information sharing and operational coordination with other Federal Government entities.
- The Office of the Director of National Intelligence is the lead coordinator for intelligence support during a significant cyber incident, acting through the Cyber Threat Intelligence Integration Center. Intelligence support and related activities include providing support to federal asset and threat agencies and facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.
- An affected federal agency shall engage in a variety of efforts to manage the impact of a cyber incident, which may include maintaining business or operational continuity; addressing adverse financial impacts; protecting privacy; managing liability risks; complying with legal and regulatory requirements (including disclosure and notification); engaging in communications with employees or other affected individuals; and dealing with external affairs (e.g., media and congressional inquiries). The affected federal agency will have primary responsibility for this line of effort.
- When a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity. The relevant sector-specific agency will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

The NCIRP builds upon these lines of effort to illustrate a national commitment to strengthening the security and resilience of networked technologies and infrastructure. This Plan outlines the structure and content from which stakeholders can leverage to inform their development of agency-, sector-, and organization-specific operational response plans. Correspondingly, this Plan should be understood to be a living document, to be updated as needed to incorporate lessons-learned, to reflect opportunities and challenges that arise as technology evolves, and to ensure the Plan adequately addresses a changing threat/hazard environment.

Introduction

The *National Cybersecurity Protection Act of 2014* (NCPA)[1] consequently codified in the *Homeland Security Act*[2], mandates that the Department of Homeland Security (DHS), in coordination with appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks to critical infrastructure. Presidential Policy Directive (PPD)-41: *U.S. Cyber Incident Coordination* and the associated Annex,[3] set forth principles governing the Federal Government's response to any cyber incident, provide an architecture for coordinating the response to significant cyber incidents, and required DHS to develop a National Cyber Incident Response Plan (NCIRP or Plan) to address cybersecurity risks to critical infrastructure. The NCIRP is part of the broader National Preparedness System and establishes the strategic framework and doctrine for a whole-of-Nation[4] approach to mitigating, responding to, and recovering from a cyber incident. This approach includes and strongly relies on public and private partnerships to address major cybersecurity risks to critical infrastructure.

- Response Plan Purpose and Organization – The NCIRP provides guidance to enable a coordinated whole-of-Nation approach to response activities and coordination with stakeholders during a significant cyber incident impacting critical infrastructure. The NCIRP sets common doctrine and a strategic framework for national, sector, and individual organization cyber operational plans.
- Intended Audience – The intended audience for the NCIRP is U.S. organizations. However, it may also enhance our international partners' understanding of the U.S. cyber incident coordination. This whole-of-Nation concept focuses efforts and enables the full range of stakeholders—the private and nonprofit sectors (including private and public owners and operators of critical infrastructure), state, local, tribal, territorial (SLTT) governments, and the Federal Government—to participate and be full partners in incident response activities. Government resources alone cannot meet all the needs of those affected by significant cyber incidents. All elements of the community must be activated, engaged, and integrated to respond to a significant cyber incident.

Scope

Cyber incident response is an important component of information and communications technology (ICT) and operational technology programs and systems. Performing incident response effectively is a complex undertaking and requires substantial planning and resources to establish a successful incident response capability.

The NCIRP is the strategic framework for operational coordination among federal and SLTT governments, the private sector, and international partners. Developed according to the guiding principles outlined in PPD-41 and leveraging doctrine from the National Preparedness System and

[1] The National Cybersecurity Protection Act of 2014. Public Law 113-282. December 18, 2014)). https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf.

[2] 6 U.S.C § 149

[3] PPD-41: *U.S. Cyber Incident Coordination*. https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident; Annex for Presidential Policy Directive-41--United States Cyber Incident Coordination, https://www.whitehouse.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident.

[4] The whole-of-Nation approach also encompasses a wide range of new and existing public and private partnerships to leverage as a platform in working towards managing cybersecurity threats and hazards to critical infrastructure.

the National Incident Management System (NIMS),[5] the NCIRP sets the strategic framework for how the Nation plans, prepares for, and responds to cyber incidents by establishing an architecture for coordinating the broader community response during a significant cyber incident in accordance with U.S. law and policy. A list of authorities is found in Annex A: Authorities and Statutes. The NCIRP is also designed to integrate and interface with industry standards and best practices for cybersecurity risk management, as developed by the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity.[6]

The NCIRP is not a tactical or operational plan for responding to cyber incidents. However, it should serve as the primary strategic framework for stakeholders when developing agency-, sector-, and organization-specific operational plans. This Plan will help those affected by cyber incidents understand how federal departments and agencies and other national-level partners provide resources to support SLTT and private sector response operations. It should also serve as the basis for national cyber operational playbooks and individual critical infrastructure sector operational coordination plans, as well as be referenced by individual entities in their own plan development. In all cases, incident response activities will be conducted in accordance with applicable law and policy.

Guiding Principles

The NCIRP is based on several guiding principles outlined in PPD-41 for the response to any cyber incident, whether involving government or private sector entities. These principles include:

- Shared Responsibility. Individuals, the private sector, and government agencies have a shared vital interest and complementary roles and responsibilities in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.
- Risk-Based Response. The Federal Government will determine its response actions and the resources it brings to bear based on an assessment of the risks posed to an entity, our national security, foreign relations, the broader economy, public confidence, privacy and civil liberties, or the public health and safety of the American people. Critical infrastructure entities also conduct risk-based response calculations during cyber incidents to ensure the most effective and efficient utilization of resources and capabilities.
- Respecting Affected Entities. To the extent permitted under law, Federal Government responders will safeguard details of the incident, as well as privacy, civil liberties, and sensitive private sector information, and generally will defer to affected entities in notifying other affected private sector entities and the public. In the event of a significant cyber incident where the Federal Government interest is served by issuing a public statement concerning an incident, federal responders will coordinate their approach with the affected entities to the extent possible.
- Unity of Governmental Effort. Various government entities possess different roles, responsibilities, authorities, and capabilities that can all be brought to bear on cyber incidents. These entities must coordinate efforts to achieve optimal results. The first federal agency to become aware of a cyber incident will rapidly notify other relevant federal agencies to facilitate a unified federal response and ensure that the right combination of agencies responds to a particular incident. When responding to a cyber incident in the private sector, unity of effort synchronizes the overall federal response, which prevents gaps in service and duplicative efforts. SLTT governments also have responsibilities, authorities, capabilities, and resources that can be

[5] NIMS. http://www.fema.gov/national-incident-management-system.

[6] Framework for Improving Critical Infrastructure Cybersecurity, version 1.0. National Institute of Standards and Technology, February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

used to respond to a cyber incident; therefore, the Federal Government must be prepared to partner with SLTT governments in its cyber incident response efforts. The transnational nature of the Internet and communications infrastructure requires the United States to coordinate with international partners, as appropriate, in managing cyber incidents.

- Enabling Restoration and Recovery. Federal response activities will be conducted in a manner to facilitate restoration and recovery of an entity that has experienced a cyber incident, balancing investigative and national security requirements, public health and safety, and the need to return to normal operations as quickly as possible.

While steady-state activities and the development of a common operational picture are key components of the NCIRP, the Plan focuses on building the mechanisms needed to respond to a significant cyber incident. Table 1 below describes the difference between a “cyber incident” and a “significant cyber incident” as outlined in PPD-41. The Federal Government uses the Cyber Incident Severity Schema (detailed in Annex B: Cyber Incident Severity Schema) to describe the incident level, the process to determine the severity of an incident, and the threshold for designating a significant cyber incident affecting the United States or its interest abroad. The United States Computer Emergency Readiness Team (US-CERT) website also provides a list of types of common ways cyber incidents can occur and exploit information and assets.[7]

Table 1: Cyber Incident Definitions from PPD-41

Incident	Definition
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.
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.

Relationship to National Preparedness System

While the NCIRP focuses on cyber incident response efforts, the National Preparedness System outlines a broader architecture that establishes how the broader community[8] prevents, protects against, mitigates, responds to, and recovers from all threats and hazards. Specifically, the National

[7] https://www.us-cert.gov/incident-notification-guidelines#attack-vectors-taxonomy

[8] The Response Federal Interagency Operational Plan, Second Edition, August 2016, describes the whole community and includes all individuals and household members, specifically inclusive of people with disabilities, children, older Americans, people with different levels of language English proficiency, communities, the private and nonprofit sectors, faith-based organizations, and local, state, tribal, territorial, insular area, and the Federal Government—and the Nation as a whole. https://www.fema.gov/media-library-data/1471452095112-507e23ad4d85449ff131c2b025743101/Response_FIOP_2nd.pdf

Response Framework (NRF)[9] sets the doctrine and provides guidance for how the Nation builds, sustains, and delivers the response core capabilities identified in the National Preparedness Goal.[10] To further connect the NCIRP with the NRF, the Homeland Security Act[11] states the Secretary of DHS, in coordination with the heads of other appropriate federal departments and agencies, and in accordance with the NCIRP under that Act, shall regularly update, maintain, and exercise the Cyber Incident Annex to the NRF of the Department. The NCIRP leverages the doctrine, capabilities, and organizing structures of the NRF, and both the NRF and NCIRP structures align with NIMS as described below.

NIMS provides the common language and incident management structure for government at all levels (federal and SLTT) and the private sector, and defines standard command and management structures. Successful response efforts, including cyber incident responses, depend on a common, interoperable approach for sharing resources, coordination, and communicating information. NIMS defines this comprehensive approach and enables the whole-of-Nation[12]to work together to prevent, protect against, mitigate, respond to, and recover from the effects of incidents regardless of cause, size, location, or complexity.

All of the components of the NIMS—resource management, management and coordination, and communications and information management—provide a common framework by which jurisdictions and organizations, which vary in authorities, management structures, communication capabilities, and protocols, integrate with one another to achieve common goals. These concepts can also apply to cyber incident response, in that they address:

- The development of a single set of incident objectives;
- The use of a collective, strategic approach to incident management;
- The improvement of information flow and coordination;
- The creation of a common understanding of joint priorities and limitations;
- The need to maintain an agency’s legal authorities; and
- The optimization of the combined efforts of all participants in the incident.

The NRF also includes 14 Emergency Support Functions (ESF)[13]; these federal coordinating structures group resources and capabilities into functional areas that are most frequently needed in a national response. ESFs are an effective way to bundle and manage resources to deliver the core capabilities outlined in the NRF. These ESFs bring together the capabilities of federal departments and agencies and other national-level assets to support incident response. The ESFs are not based on

[9] The NRF is one of five frameworks in the National Preparedness System; it describes how the whole community works together to achieve the National Preparedness Goal within the Response mission area. http://www.fema.gov/national-response-framework.

[10] http://www.fema.gov/national-preparedness-goal.

[11]6 U.S.C. § 149

[12] The National Preparedness System refers to whole community vs the NCIRP describing a whole-of-Nation approach because of the nature of cyber infrastructure and associated incidents. The guidance, programs, processes, and systems that support each component of the National Preparedness System enable a collaborative, whole community approach to national preparedness that engages individuals, families, communities, private and nonprofit sectors, faith-based organizations, and all levels of government. https://www.fema.gov/media-library-data/20130726-1855-25045-8110/national_preparedness_system_final.pdf

[13] http://www.fema.gov/national-preparedness-resource-library.

the capabilities of any single department or agency but are groups of organizations that work together to support an effective response.

Activation of the ESFs, either by the DHS Federal Emergency Management Agency (FEMA) or as directed by the Secretary of Homeland Security, depends upon the response activities needed to support the incident. Specifically, through ESF #2 (Communications), the Federal Government can coordinate the response to and recovery from a significant cyber incident that also creates large-scale physical effects with the communications sector and across the other ESFs. In an incident with cyber and physical effects, the significant cyber incident response mechanism outlined in the Coordinating Structures and Integration section of this Plan will coordinate with the established ESFs, to include ESF #2. A graphic comparing the Cyber Incident Severity Schema and Activation Level of the National Response Coordination Center is provided in Annex C. This center is a multiagency center that coordinates the overall federal support for major incidents and emergencies.[14]

The next section describes the concurrent lines of effort outlined in PPD-41 and identifies key roles and responsibilities for not only the federal and SLTT governments' response but also the private sectors' response to a cyber incident as they own and operate the bulk of the Nations' critical infrastructure.

Roles and Responsibilities

Every day, various organizations across the public and private sectors manage, respond to, and investigate cyber incidents through concurrent lines of effort. Fostering unity of effort during incident response requires a shared understanding of the roles and responsibilities of all participating organizations, to include roles that may be unique or particularly relevant for protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.

The Federal Government maintains a wide range of capabilities and resources that may be required to respond to a cyber incident, many of them through its cybersecurity centers which are further described in Annex E: Roles of Federal Cybersecurity Centers. In responding to any cyber incident and recognizing the shared responsibility for cybersecurity, the Federal Government organizes its' response activities based upon four concurrent lines of effort: threat response, asset response, intelligence support, and the affected entity's internal response activities.

When a cyber incident affects a private entity, the Federal Government will typically not play a direct role in the affected entities' response activities but will remain cognizant of their activities and coordinate appropriately with the affected entity. Where possible, and especially where incidents may escalate on the Cyber Incident Severity Schema, the Federal Government will conduct coordinated outreach efforts with the affected entity and offer to assist with asset response, threat response, and intelligence support activities, consistent with the guiding principles described in the Scope section of this Plan.

Cyber incidents can result from the actions, or inactions, of a single individual. When engaged and educated, individuals, families, and households can greatly reduce the impact, disruption, and damage caused by a cyber event. While most cyber incidents may not involve assistance from private citizens, incidents can reduce the risk and potential impact of a cyber incident to their personal property. Resources and guidance are available at www.ready.gov/cyber-attack that private citizens

[14] The National Response Coordination Center. https://www.fema.gov/media-library-data/1440617086835-f6489d2de59dddeba8bebc9b4d419009/NRCC_July_2015.pdf

can leverage before, during, and after a cyber incident. US-CERT also provides information to home users on security risks and countermeasures associated with home Internet connectivity.[15]

Concurrent Lines of Effort

Recognizing the shared responsibility for cybersecurity, response activities in the NCIRP are undertaken through three concurrent lines of effort: threat response, asset response, intelligence support and related activities. A fourth line of effort is the affected entity's response efforts.[16] These concurrent lines of effort provide a foundation for harmonizing various response efforts and fostering coordination and unity of effort before, during, and after any cyber incident response. Federal and non-federal entities should remain cognizant of these lines of effort and facilitate their activities accordingly while responding to cyber incidents.

Table 2. Lead Federal Agencies During Significant Cyber Incidents Affecting Civilian Networks[17]

Line of Effort	Lead Federal Agency
Threat Response	Department of Justice (DOJ) through the Federal Bureau of Investigation (FBI) and National Cyber Investigative Joint Task Force (NCIJTF)
Asset Response	Department of Homeland Security (DHS) through National Cybersecurity and Communications Integration Center (NCCIC)
Intelligence Support	Office of the Director of National Intelligence (ODNI) through Cyber Threat Intelligence Integration Center (CTIIC)
Affected Entity Response	When a significant cyber incident affects a federal agency, that agency will have primary responsibility for its response. When a significant cyber incident affects a private entity, the Federal Government will typically not play a role in this line of effort, but the cognizant Sector Specific Agency(ies) will generally coordinate the Federal Government efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

Threat and asset responders share some responsibilities and activities, including but not limited to:

- Communicating with the affected entity to understand the nature of the cyber incident;
- Providing guidance to the affected entity on available federal resources and capabilities;
- Promptly disseminating, through appropriate channels, intelligence and information learned in the course of the response; and
- Facilitating information sharing and operational coordination with other entities.

International coordination plays a key role through all the lines of effort. Due to the transnational nature of the Internet and communications infrastructure, and the global presence and connectivity of

[15] https://www.us-cert.gov/Home-Network-Security

[16] PPD-41: U.S. Cyber Incident Coordination. https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[17] Per the Annex to PPD-41, asset and threat response activities for significant cyber incidents affecting DoD or IC assets are led by those agencies with support from other federal agencies as appropriate. Lead agencies also coordinate with relevant SSAs, if a cyber incident affects or is likely to affect sectors they represent.

the U.S. private sector, the Federal Government may coordinate with international partners in response to all aspects of a cyber incident—threat response, asset response, and intelligence support.

The Department of State (DOS) represents the United States in all global diplomatic engagements across the full range of international policy imperatives, including cyber issues. As stated in the 2011 International Strategy for Cyberspace, diplomacy is a vital and necessary component to addressing cyber threats and responding to cyber incidents both domestically and internationally. DOS leverages its diplomats in the embassies and posts around the globe to provide international diplomatic support for cyber incident response around the clock. While DOS coordinates diplomatic outreach related to cyber incidents, many federal departments and agencies actively maintain and leverage multilateral and bilateral partnerships. Similarly, many ICT sector businesses and providers are multinational businesses with critical international elements and relationships, including interaction with both policy and operational communities around the world. As appropriate, federal departments and agencies collaborate internationally and with private sector entities to support international aspects of cyber incident response.

Threat Response

Threat response activities encompass many resources and capabilities from across the law enforcement and defense community. Threat response activities during a cyber incident include investigative, forensic, analytical, and mitigation activities; interdiction of a threat actor; and providing attribution that may lead to information sharing and operational synchronization with asset response activities. Threat response activities also include conducting appropriate law enforcement and national security investigative activities at the affected entity’s site, linking related incidents, and identifying additional affected or potentially affected entities. As described earlier, threat responders and asset responders collaborate to foster a unity of effort to facilitate their activities while responding to incidents. The SLTT community and the private sector play important roles in working with respective law enforcement entities on threat response activities. Federal agencies with counterintelligence functions, such as those of DHS, DOJ, DoD, Department of Energy (DOE), and members of the Intelligence Community (IC), may perform a substantial threat response role when a significant cyber incident affects their duties or responsibilities, or there is suspicion of activities conducted a foreign power or agent of a foreign power.

Private Sector

Private sector entities perform critical roles in supporting threat response activities by reporting and sharing information regarding cyber incidents and malicious cyber activity in a timely manner to appropriate law enforcement agencies or government entities. Information, communications, and technology providers and manufacturers—such as Internet service providers, common carriers, manufacturers of key networking hardware, and major software companies—also play an important role in the threat response to malicious cyber activity, due to the potential exploitation or use of their systems by cyber threat actors. Points of contact for reporting incidents to Federal Government entities are provided in Annex D: Reporting Cyber Incidents to the Federal Government. Private sector entities should also adhere to regulatory and legal requirements when reporting cyber incidents. Private sector cybersecurity practitioners and providers that offer critical services (such as managed security services, indications and warning, cybersecurity assessment, and incident response) may also possess information concerning malicious cyber activity that is important to enable threat response activities. The *Cybersecurity Information Sharing Act of 2015* provides liability and other legal protections to private sector and certain SLTT government organizations and establishes important conditions regarding sharing information with the Federal Government, SLTT government organizations, and the private sector.[18]

State, Local, Tribal, and Territorial Governments

Many states and locals have criminal statutes regarding unauthorized access or damage to computer systems, which could be implicated in a cyber incident. State fusion centers are situated at the intersection between federal and local law enforcement, and play a role in sharing threat-related information between federal, SLTT and/or private sector partners. However, state fusion centers vary greatly in their cyber capacity and capability. Local governments, particularly large cities, play an important role in local response activities. Often times, private citizens and small businesses do not have relationships with or access to federal law enforcement or in incident response activities. Local governments have a critical responsibility to provide a communication bridge to federal and state law enforcement and incident responders. As identified in the previous sub-section (Private Sector), the *Cybersecurity Information Sharing Act of 2015* establishes legal protections and important conditions for sharing information with the Federal Government, SLTT government organizations, and the private sector.

Federal Government

In response to cyber incidents, federal law enforcement agencies work across SLTT and the Federal Government, international engagements, and with private sector entities to address both criminal and national security cyber threats. Federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI), United States Secret Service (U.S. Secret Service), and U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), conduct threat response activities related to criminal activity involving their investigative jurisdictions and coordinate appropriately. Sharing action information in an unclassified format between the IC and first responders is critical in coordinating incident response activities.

Pursuant to PPD-41, during the event of a significant cyber incident for which a Cyber Unified Coordination Group (UCG) is convened, the DOJ, through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), will serve as the lead federal agency for threat response activities. The specific responsibilities and coordinating roles for this line of effort during a significant cyber incident are detailed in the Operational Coordination During a Significant Cyber Incident section of this Plan.

DOJ's Offices of U.S. Attorneys and its' Criminal and National Security Divisions, working with federal law enforcement agencies, use criminal and national security authorities to investigate, prosecute, and disrupt cyber threats and to apprehend cyber threat actors. Information and evidence obtained pursuant to appropriate legal process are used to identify the source of cyber incidents and to gather pertinent cyber threat information. Nationwide coordination of cyber prosecutorial initiatives is conducted through the DOJ Computer Hacking and Intellectual Property Program for criminal matters and by the DOJ National Security Cyber Specialist Network for cyber threats to the national security. In addition, DOJ, through the FBI and NCIJTF, shares investigative information and cyber threat intelligence, as appropriate, with other federal agencies to aid in the analysis of cyber threats and vulnerabilities. The FBI Cyber Task Forces in all 56 field offices support SLTT

[18] Further information and guidance to assist non-federal entities to share cyber threat indicators and defensive measures with federal entities under the Cybersecurity Information Sharing Act of 2015 can be found at https://www.us-cert.gov/ais.

law enforcement in maintaining relationships and sharing information with the private sector, offering training and certification courses, and coordination of domestic cyber threat investigations.

The U.S. Secret Service has a national network of Electronic Crimes Task Forces, which combine the resources of academia, the private sector, and SLTT law enforcement to prevent, detect, and investigate electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

DoD is responsible for threat response to cyber incidents affecting DoD assets and the DoD Information Network (DoDIN). DoD can also support civil authorities for cyber incidents outside the DoDIN when requested by the lead federal agency, and approved by the appropriate DoD official, or directed by the President. Such support would be provided based upon the needs of the incident, the capabilities required, and the readiness of available forces.

Asset Response

Asset response activities include furnishing technical assistance to affected entities, mitigating vulnerabilities, identifying additional at-risk entities, and assessing their risk to the same or similar vulnerabilities. These activities could also include communicating with the affected entity to understand the nature of the cyber incident; providing guidance to the affected entity on available federal, SLTT, and private sector resources and capabilities; promptly disseminating new intelligence and information through the appropriate channels; and facilitating information sharing and operational coordination with other Federal Government, SLTT government, and private sector entities. Critical asset response activities also include assessing potential risks to a sector or region, including potential cascading and interdependency effects, developing courses of action to mitigate these risks, and providing guidance on how best to utilize federal, SLTT, and private sector resources and capabilities in a timely, effective manner.

Asset and threat responders coordinate and share some responsibilities and activities when responding to a cyber incident. The roles and responsibilities in asset response vary, which highlights that unity of effort and shared responsibility is necessary to protect the Nation against cyber incidents.

Private Sector

The private sector, especially the owners and operators of critical infrastructure, plays a key role in responding to cyber incidents. Small, medium, and large private sector entities are often the first and primary responders to cyber incidents. Private companies are responsible for the security of their own systems, and they are normally the first to identify an incident and are often in the best place to respond to it. Private entities may have reporting or disclosure requirements related to cyber incidents, which they have to comply with as they respond to the incident. In most cases, these incidents are considered routine and are mitigated by the company using internal resources or with the assistance of contracted services providers. Routine, steady-state information sharing related to cyber incidents, even when mandatory reporting is not required, alerts other at-risk entities and allows them to mitigate vulnerabilities that may have cascading impacts to their systems.

Private sector service providers and cybersecurity practitioners offer critical services, such as managed security services, indications and warning, cybersecurity assessment, and incident response, which system owners and other asset responders might need when managing an incident. These private sector resources can serve as surge and specialty support to augment an in-house cybersecurity team at an affected entity.

Information, communications, and technology providers and manufacturers, such as Internet service providers, other common carriers, manufacturers of key networking hardware, and major software companies, play an important role in defending against and responding to malicious cyber activity. Effective coordination between these private sector entities and other response organizations is often essential in cyber incident response.

Critical infrastructure owners and operators work with DHS and relevant sector-specific agencies (SSA) implementing the National Infrastructure Protection Plan (NIPP)[19] tenets of public-private partnership to improve preparedness and manage risk. Due to the tightly interconnected and interdependent nature of some sectors, companies may also provide information to other entities in the sector or in other sectors, to facilitate shared situational awareness, contain the incident, and/or mitigate any damage. Thus, companies will potentially look to share and receive information from a variety of sources including DHS, SSAs, and federal and SLTT law enforcement and counterintelligence activities as well as their respective sector Information Sharing Analysis Centers (ISAC) and other information sharing and analysis organizations.

Most private sector operational information sharing is conducted through ISACs. ISACs are typically a sector-based type of Information Sharing and Analysis Organization (ISAO) and operate through a defined sector-based model, meaning that organizations within a certain sector (i.e. financial services, energy, aviation, etc.) join together to share information about cyber threats. Although many of these groups are already essential drivers of effective cybersecurity collaboration, some organizations do not fit neatly within an established sector or have unique needs. ISAOs can be formed based upon geography, sector, or any other grouping in which companies are interested and is a group created to gather, analyze, and disseminate cyber threat information. Those organizations that cannot join an ISAC but have a need for cyber threat information could benefit from membership in an ISAO. Unlike ISACs, ISAOs are not necessarily tied to critical infrastructure sectors.[20]

In the case of cyber incidents, especially significant cyber incidents, greater coordination may be needed with the Federal Government, SLTT communities, regulators within the sector, and among multiple sectors. In addition to responding to situations in which private companies are themselves the victims of cyber incidents, private entities also respond to situations in which private sector service providers (especially Internet service providers, managed security service providers, and other technology vendors) provide support for national-level incident response efforts. During such an incident, the private sector often provides support or assistance to federal and SLTT departments and agencies on preparedness and response activities. Federal and SLTT regulators also have mandatory reporting requirements for certain types of cyber incidents in certain sectors. Depending on the sector and type of incident, some response actions may require regulator coordination, approval, and/or regulatory relief.

As appropriate, private sector entities provide for the security of their networks and security processing of breaches or other incidents through standing in-house or contracted services or use of external experts. Standing services are a part of the entity's network structure, and the private sector entity are encouraged share with government responders the information the standing services develop or pursue concerning a cyber incident. The *Cybersecurity Information Sharing Act of 2015* provides liability and other legal protections to private sector and certain SLTT government organizations and establishes important conditions regarding sharing information with the Federal Government, SLTT government organizations, and the private sector.[21]

[19] NIPP, 2013. https://www.dhs.gov/national-infrastructure-protection-plan.

[20] https://www.dhs.gov/isao-faq

[21] Further information and guidance to assist non-federal entities to share cyber threat indicators and defensive measures with federal entities under the Cybersecurity Information Sharing Act of 2015 can be found at https://www.us-cert.gov/ais.

State, Local, Tribal, and Territorial Government

Ensuring the safety and welfare of citizens is a fundamental responsibility of government at every level. Toward these objectives, key executives, executive leadership, elected officials, and executive staff of each SLTT government are responsible for ensuring preparedness, response, and recovery activities within their jurisdiction.

In cases of cyber incidents, the standard emergency response roles and responsibilities may not be sufficient to address technical challenges. Each state is responsible for developing a plan that describes their role in asset response for entities within their state. This state plan should be consistent with the NCIRP and serve as a cyber annex to their respective state emergency management plan. Information described in Annex G: Developing an Internal Cyber Incident Response Plan provides information each state can consider when developing a cyber incident response plan that coordinates identifying, detecting, mitigating, responding to, and recovering from cyber incidents in their state.

In establishing strong governance and reporting mechanisms, executives should identify key individual response points-of-contact for their respective governments and ensure the Federal Government has the most up-to-date information for these individuals. To facilitate coordination during a significant cyber incident response operation, each key executive should pre-designate a primary individual to serve as Senior Official to represent its government. Until amended, by each key executive, the NCCIC uses the state Homeland Security Advisors as its primary point of contact.

Governance is vital and an enabling factor in states' cyber asset response role. This includes the supporting legal framework, policies, plans, and procedures that codify the state chief information security officer's authorities and responsibilities. Governance also outlines how these relate to executive branch departments and agencies, and other state-operated entities to include (and not limited to) state and local emergency management functions, law enforcement, the judicial and legislative branches, ports, airports, and other state owned critical infrastructure. As identified in the previous sub-section (Private Sector), the *Cybersecurity Information Sharing Act of 2015* establishes legal protections and important conditions for sharing information with the Federal Government, SLTT government organizations, and the private sector.

Resources available to SLTT communities include, but are not limited to, the following:

- Regional Homeland Security Offices and Fusion Centers;
- Multi-State ISAC (MS-ISAC) is funded through grants from DHS to support the security of the SLTT government networks[22] and acts as a focal point for critical information exchange and coordination between the SLTT community and the Federal Government; every state has an MS-ISAC primary member, usually the state chief information security officer (CISO);
- Local governments that are eligible to apply and receive Urban Area Security Initiative grant funds are encouraged to include cybersecurity and training programs as part of their expenditures.
- DHS National Protection and Programs Directorate field personnel, including:

[22] The MS-ISAC does not help SLTT governments who are seeking to support the private sector. If an SLTT government is supporting a private sector company in asset response, the SLTT government should engage directly with the NCCIC.

    - Supervisory, regional, and district-level Cybersecurity Advisors, who work closely with SLTT Chief Information Security Officers and cyber emergency management communities as cybersecurity subject matter experts;
    - Regional directors and Protective Security Advisors, who work closely with state homeland security advisors as critical infrastructure protection specialists;
- The Governors Homeland Security Advisors Council, which provides a structure through which homeland security advisors from each state, territory, and the District of Columbia discuss homeland security issues, share information and expertise, and keep governors informed of the issues affecting homeland security policies in the states;
- The SLTT Government Coordinating Councils (SLTT GCC), which strengthen the sector partnership structure by bringing together geographically diverse experts from a wide range of critical infrastructure disciplines to ensure that SLTT officials play an integral role in national critical infrastructure security and resilience efforts.

The National Guard is a force with dual state and federal roles. National Guard forces have expertise in critical response functions and many also have expertise and capabilities in cyber activities. At the direction of a State Governor and Adjutant General, the National Guard may perform state missions, including supporting civil authorities in response to a cyber incident. In certain circumstances, as permitted by law, the National Guard may be requested to perform federal service or be ordered to active duty to perform DoD missions, which could include supporting a federal agency in response to a cyber incident.

Following a cyber incident, SLTT community leaders and points of contact may be asked to provide advice, support, and assistance to federal departments and agencies on preparedness and response activities related to SLTT priorities. Cyber incidents can cause cascading and/or physical impacts that implicate non-cyber incident response activities by SLTT governments. Key executives and points of contact have a need for situational awareness of the Federal Government's asset response activities even when a cyber incident does not affect the SLTT government systems. They should be prepared to request additional resources from the Federal Government—for instance, under the Stafford Act—in the event of a cyber incident that exceeds their government's capabilities.

Federal Government

Federal asset response to a significant cyber incident encompasses many resources and capabilities from across the federal departments and agencies as well as with the private sector. In response to cyber incidents, the Federal Government works with both domestic and foreign partners, including both private sector and governmental entities, to assist in assessments, mitigation, recovery, and restoration activities. Pursuant to PPD-41, in the event of a significant cyber incident for which a Cyber UCG is convened, DHS, through the NCCIC, will serve as the lead federal agency for asset response activities. The specific responsibilities and coordinating roles for this line of effort during a significant cyber incident are detailed in the Operational Coordination During a Significant Cyber Incident section of this Plan.

The Office of Management and Budget and the Federal Information Security Modernization Act of 2014 directs federal departments and agencies to report major cyber incidents within seven days as well as submitting to Congress, DHS, and Office of Management and Budget on an annual basis.[23]

[23] Federal Information Security Modernization Act of 2014. Public Law No: 113-283. December 18, 2014. https://www.congress.gov/bill/113th-congress/senate-bill/2521

DHS, through the US-CERT, must be notified of all computer security incidents involving a Federal Government information system with a confirmed impact to confidentiality, integrity, or availability within one hour of being positively identified by the agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center, or Information Technology department.[24]

DHS provides strategic guidance, promotes a national unity of effort, and coordinates the overall federal effort to promote the security and resilience of the Nation's critical infrastructure from cyber and other threats.[25] Per the NCPA, DHS, through the NCCIC, serves as the federal civilian interface for sharing information related to cybersecurity risks, incidents, analysis, and warnings for federal and non-federal entities.[26] The NCCIC facilitates information sharing to help identify other entities at risk to the same or similar vulnerabilities and shares mitigation recommendations and best practices to protect those at risk. The NCCIC closely coordinates with the SSAs, representatives from multiple agencies, and the private sector to share cybersecurity information, information about risks and incidents, analysis, and warnings among federal and non-federal entities, and to facilitate coordination regarding cybersecurity risks and incidents across the civilian communities, SLTT governments, and the private sector. Federal asset response support to the private sector from the NCCIC in the form of on-site technical assistance is generally contingent on a request from or consent of the supported entity.

SSAs also play a role in sector coordination, working closely with DHS and serving as a day-to-day federal interface to prioritize and coordinate activities within their respective sectors; carrying out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations; and providing support or facilitating technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate. DHS ensures consistent and integrated approaches across various critical infrastructure sectors, and a nationwide approach including both unity of effort and unity of messages.

DHS, working with relevant SSAs, also coordinates the Government's efforts to understand the potential business or operational impact of a cyber incident on critical infrastructure in a given sector and across sectors. The relevant SSA will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure. SSAs receive support from the DHS NCCIC and the National Infrastructure Coordinating Center to maintain and provide situational awareness on threats, incidents, or events impacting critical infrastructure and to facilitate information sharing. This includes a near-real-time capability to provide SSA reports, coordinated with FEMA ESF reporting provided by the National Response Coordination Center, and the capability to solicit and receive information on incidents from public and private sector critical infrastructure partners. Because SSAs often have authorities, responsibilities, and partnerships with private industry that extend beyond security and resilience issues, SSAs play a lead role in integrating response to the technical aspects of cybersecurity incidents with efforts to mitigate the systemic impacts of such incidents to sectors.

[24] US-CERT Federal Incident Notification Guidelines. https://www.us-cert.gov/incident-notification-guidelines

[25] Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. February 12, 2013. PPD-12 also assigns roles and responsibilities to other federal agencies. The Department of Justice and Federal Bureau of Investigation lead counterterrorism and counterintelligence investigations and related law enforcement activities across critical infrastructure. The Department of Homeland Security and the Attorney General collaborate to carry out their respective missions in critical infrastructure. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[26] The National Cybersecurity Protection Act of 2014. Public Law 113-282. December 18, 2014. http://www.gpo.gov/fdsys/pkg/PLAW-113publ282/pdf/PLAW-113publ282.pdf.

In responding to cyber incidents, DHS also works with foreign partners to exchange information and coordinate incident response activities. This international coordination principally occurs between the NCCIC and its foreign government CSIRT counterparts and builds on regular information sharing and operational coordination relationships. The DOC coordinates with federal, international, and private sector partners on the impacts of cyber incidents on the Internet ecosystem: the domain name system and the digital economy platform representatives to assess those impacts. Through the National Telecommunications and Information Administration and NIST, DOC serves as the Nation's authority on cybersecurity risk management practices and also fulfills responsibilities under the Defense Production Act[27] through the Bureau of Industry and Security, including support to critical infrastructure.

In some cases, regulatory or contract requirements could impose certain obligations on the affected entity related to asset response support, such as mandatory reporting requirements and/or national security determinations that may override normal consultative processes. Additionally, where they have relevant authority, federal regulators should be engaged early in the incident response process to ensure that actions requiring waiver or other approval or notification can be quickly executed. Regulators may also be able to facilitate coordinated actions of their respective sectors as necessary during significant cyber incidents.

DoD will be responsible for managing the asset response affected military assets and the DoDIN. DoD can also support civil authorities in responding to cyber incidents outside the DoDIN through a Defense Support of Civil Authorities request based upon a request by the lead federal agency and approved by the appropriate DoD official or directed by the President. Support would be provided based on the needs of the incident, the capabilities required, and the readiness of available forces.

When incidents affect IC assets, the IC Security Coordination Center (IC SCC) is responsible for asset response. The Office of the Director of National Intelligence (ODNI) manages the threat and asset response for the integrated defense of the IC information environment through the IC SCC, in conjunction with IC mission partners and with support from other federal agencies, as appropriate.

Intelligence Support

Intelligence and related supporting activities play an important role to better understand the cyber incident and existing targeted diplomatic, economic, or military capabilities to respond and share threat and mitigation information with other potential affected entities or responders. Especially during a significant cyber incident, asset and threat responders should leverage intelligence support activities as necessary to build situational threat awareness; share related threat indicators and analysis of threats; identify and acknowledge gaps; and ultimately create a comprehensive picture of the incident.

State, Local, Tribal, and Territorial Government

States fusion centers involve various levels of state government, private sector entities, and the public—though the level of involvement of some of these participants will vary based on specific circumstances. The fusion process should be organized and coordinated, at a minimum, on a statewide level, and each state should establish and maintain a center to facilitate the fusion process. Though the foundation of fusion centers is the law enforcement intelligence component, center leadership should evaluate their respective jurisdictions to determine what public safety and private sector entities should participate in the fusion center.

[27] Defense Production Act of 1950, as Amended October 2009. (50 U.S.C. App. 2061 et seq.) https://www.fema.gov/media-library/assets/documents/15666

Federal Government

ODNI, through the Cyber Threat Intelligence Integration Center (CTIIC), provides intelligence support to federal agencies in response to cyber incidents. Pursuant to PPD-41, in the event of a significant cyber incident for which a Cyber UCG is convened, ODNI, through CTIIC, will serve as the lead federal agency for intelligence support and related activities. The specific responsibilities and coordinating roles for this line of effort during a significant cyber incident are detailed in the Operational Coordination During a Significant Cyber Incident section of this Plan.

In this role, CTIIC coordinates development of federal intelligence information for the other federal cybersecurity centers and federal stakeholders. This could include pursuing declassification of intelligence and/or “tear-line” reports at different classification levels as appropriate to the circumstances of the incident and overall U.S. equities. CTIIC also coordinates any intelligence collection activities that may take place as part of the incident through the National Intelligence Manager for Cyber.

Each intelligence operational center has its own organic intelligence support that aligns to its operational responsibilities. The DHS Office of Intelligence and Analysis has responsibilities under Title 6[28] to deliver intelligence to SLTT and private sector partners and develop intelligence from those partners for the Department and the IC. In addition, it provides intelligence support to the NCCIC’s private sector information sharing mission including gathering intelligence requirements from critical private sector companies and if the DHS National Protection and Programs Directorate concurs with the requirements can submit as formal requirements into the intelligence process.

The FBI collects and coordinates the sharing of relevant intelligence and other information between FBI domestic personnel and FBI staff assigned to Legal Attaché offices around the world; coordinates the sharing of intelligence among and between federal agencies and international intelligence and law enforcement elements; produces and shares analytical products, including those that assess threats to the homeland and inform related planning, capability development, and operational activities; and coordinates with ODNI mission and support centers that provide unique capabilities for homeland security partners.[29]

The National Security Agency Cybersecurity Threat Operations Center (NCTOC) is the 24/7/365 NSA element that characterizes and assesses foreign cybersecurity threats. The NCTOC informs partners of current and potential malicious cyber activity through its analysis of foreign intelligence, with a focus on adversary computer network attacks, capabilities, and exploitations. Upon request, the NCTOC also provides technical assistance to U.S. Government departments and agencies.

The DoD actively characterizes and assesses foreign cybersecurity threats and informs the relevant interagency partners of current and potential malicious cyber activity. Upon request, the DoD intelligence components may provide technical assistance to U.S. Government departments and agencies; other DoD elements may provide support to civil authorities in accordance with applicable law and policy. The IC may identify classified information, indicating a potential credible cyber threat to an SLTT, critical infrastructure owner/operator, or other private sector entity. In accordance with Section 4 of Executive Order 13636, DHS and/or the FBI provide appropriate notification to the targeted entity.[30] Where available, declassified threat detection and mitigation information may also be provided. In circumstances where the source of threat identification, nature of the adversary, or

[28]6 U.S.C. §124a.

[29] Title II of the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, 118 Stat. 3638, outlines FBI intelligence authorities, as does Executive Order 12333; 50 U.S.C. 401 et seq.; 50 U.S.C. 1801 et seq."

[30] The NCIJTF has implemented the EO 13636 4(b) tracking system, Cyber Guardian, to record the production, dissemination, and disposition of these notifications.

other factors of national security concern exist, incident response processes and procedures adhere to all guidelines and directions for handling matters of national security.

Affected Entity's Response

Entities affected by a significant cyber incident usually undertake activities to manage the effects of the cyber incident on its operations, customers, and workforce, to include complying with various legal, regulatory, or contractual obligations. When a federal agency is an affected entity, that agency has primary responsibility for engaging in a variety of efforts to manage the impact of the cyber incident. These efforts could include, but not limited to:

- Maintaining business or operational continuity;
- Mitigating potential health and safety impacts;
- Addressing adverse financial impacts;
- Protecting privacy;
- Managing liability risk;
- Complying with legal and regulatory requirements (including disclosure and notification);
- Engaging in communications with employees or other affected individuals; and
- Managing external affairs (e.g., media and congressional inquiries).

When a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity. The relevant SSA will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

Cyber Incidents Involving Personally Identifiable Information

As it relates to cyber incidents affecting civilian Federal Government agencies, if the facts and circumstances lead to a reasonable suspicion that the known or suspected cyber incident involves personally identifiable information, then the appropriate senior agency officials for privacy will be notified and lead any necessary personally identifiable information incident response process, as required by the Office of Management and Budget Memorandum M-07-1612, *Safeguarding Against and Responding to the Breach of* Personally Identifiable Information (and its subsequent revisions), and the agency's Breach Response Plan.[31]

Core Capabilities

Core capabilities are the distinct critical elements needed to conduct the threat response, asset response, and intelligence support activities in response to a cyber incident. Core capabilities are the activities that generally must be accomplished in cyber incident response, regardless of which levels of government are involved. They provide a common vocabulary to describe the significant functions that must be developed and executed across the whole-of-Nation to ensure preparedness.

[31] Office of Management and Budget Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information. May 22, 2007. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

Core capability application may be achieved with any combination of properly planned, organized, and trained personnel and deployed through various approaches such as the NIST Cybersecurity Framework or cybersecurity activities developed by the private sector. The National Preparedness Goal organizes the core capabilities into mission areas. These capabilities are aligned in Annex H: Core Capability/NIST Cybersecurity Framework/PPD-41 Crosswalk.

The capabilities are briefly described in this section and in further detail in Annex F: Core Capabilities and align with the National Preparedness Goal core capabilities.[32] While Annex F is not an exhaustive list of capabilities, it provides a description of the capabilities that should be developed and utilized for particular needs, and roles, responsibilities, and authorities for the nature and scope of the cyber incident. All levels of government, private and non-profit sector organizations, and critical infrastructure owners and operators should assess their particular risks to identify their core capability requirements. Annex I describes additional resources that can be leveraged by both the private and public sector. Those resources can also serve as a starting point for understanding cyber incident response, vulnerability updates, data breach information, risk management, and organizations.

Responding to a cyber incident, like incident response for all other threats and hazards, is a shared responsibility. The whole-of-Nation must work together to ensure the United States is optimally prepared for cyber incidents; recognizing that not every network/system faces the same risks. By engaging the whole-of-Nation to build and deliver the cyber response core capabilities, the Nation is better prepared to respond to any threat or hazard, assist in restoring basic services and community functionality, and facilitate the integration of recovery activities.

Access Control and Identity Verification

Description: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems, which is also referred to as Authentication and Authorization. This capability relies on the implementation and maintenance of protocols to verify identity and authorize, grant, or deny access to specific IT systems and networks.

Cybersecurity

Description: Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorized use, and exploitation. More commonly referred to as information security, these activities ensure the security, reliability, confidentiality, integrity, and availability of critical information, records, and communications systems and services through collaborative initiatives and efforts.

Forensics and Attribution

Description: Forensic investigations and efforts to provide attribution for an incident are complementary functions that often occur in parallel during a significant cyber incident.

Forensics: Forensics is the term for discovering and identifying information relevant to an investigation through both scientific and intelligence-based acumen. In the context of a cyber incident, forensics refers to a number of technical disciplines related to the duplication, extraction, and analysis of data to uncover artifacts relevant to identifying malicious cyber activity. Forensics includes several sub-disciplines, including host-based forensics, network and packet data forensics,

[32] https://www.fema.gov/core-capabilities

memory analysis, data correlation, and malware analysis.

During the response to a significant cyber incident, government agencies and private sector partners frequently conduct simultaneous analysis and share analytical results with each other to create a common understanding regarding the malicious cyber activity and how to defend against these or similar activity. In the days following an incident, a number of different threat, asset, and business response organizations may also engage in simultaneous forensic analysis. Although these lines of effort may appear to be duplicative, findings from these efforts could vary depending on the entities' varied access to particularized datasets or holdings.

Attribution: Attribution identifies an adversary linked to a particular incident. It is the culmination of the review of evidence and intelligence gathered during an incident which results in an assessment that identifies individuals or organizations which likely played a role in the cyber incident.

Attribution occurs over the lifecycle of an investigation and may not be known at the onset of a cyber incident response. Although the development of attribution for a significant cyber incident is one of the primary functions of lead federal response agencies, other government and private sector entities have a significant role to play in determining attribution.

An assessment regarding attribution for an incident is not only important for government agencies conducting criminal or national security investigations; it could also be significant to an affected entity as it considers whether to pursue additional legal or civil action against threat actors.

This core capability also includes unique and technical activities that support computer network and asset analysis during an incident. These supporting activities contribute to awareness of a comprehensive picture, which ultimately helps reduce the impact of a current incident and prevent future cyber incidents from spreading across the network.

Infrastructure Systems

Description: Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity. Critical infrastructure and cyber networks are interdependent. In a response to a cyber incident, this capability focuses on stabilizing the infrastructure assets and entities, repairing damaged assets, regaining control of remote assets, and assessing potential risks to the critical infrastructure sector at large.

Intelligence and Information Sharing

Description: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as necessary.

In the context of a cyber incident, this capability involves the effective implementation of the intelligence cycle and other information collection and sharing processes by federal and SLTT entities, the private sector, and international partners to develop situational awareness of potential cyber threats to the United States.

Interdiction and Disruption

Description: Delay, divert, intercept, halt, apprehend, or secure threats related to malicious cyber activity. In the context of a cyber incident, these threats include people, software, hardware, or activities that pose a threat to the Nation's cyber networks and infrastructure. This includes those interdiction and disruption activities that may be undertaken in response to specific, actionable intelligence of a cyber threat. Interdiction and disruption may include the targeting of persons, programs, or equipment or machines to stop or thwart threat activities and employing technical and other means to prevent malicious cyber activities. Interdiction and disruption capabilities help thwart emerging or developing cyber threats and neutralize operations. These capabilities should be utilized in a manner that preserves evidence and the Government's ability to prosecute those who violate the law.

Logistics and Supply Chain Management

Description: Facilitate and assist with delivery of essential commodities, equipment, and services in support of responses to systems and networks impacted by malicious cyber activity. Synchronize logistics capabilities and enable the restoration of impacted supply chains.

In the context of a cyber incident, this capability focuses on providing the logistical or operational support to achieve cyber incident response priorities established by leadership through identifying, prioritizing, and coordinating immediate response resource requirements.

Operational Communications

Description: Ensure the capacity for timely communications in support of security, situational awareness, and operations, by any and all means available, among and between entities affected by the malicious cyber activity and all responders.

In the context of a cyber incident, this capability includes identifying federal support organizations, capabilities, and teams with internal interoperable voice, video, and data systems and networks essential for effective cyber incident response operations. In a cyber incident, this capability focuses on the timely, dynamic, and reliable movement and processing of incident information in a form that meets the needs of decision makers at all levels of government and authorized participating private sector partner organizations.

Operational Coordination

Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrate all critical stakeholders and support execution of core capabilities. This is the capability to conduct actions and activities that enable decision makers across the whole-of-Nation to determine appropriate courses of action and to provide oversight for complex operations, to achieve unity of effort and effective outcomes. Operational coordination, in accordance with the principles of the NIMS and the Incident Command System, coordinates the threat response, asset response, and intelligence support activities in the face of a cyber threat or in response to an act of terrorism committed in the homeland. Unity of message is included within the guiding principles. Further information is available in Annex D: Reporting Cyber Incidents to the Federal Government.

In the context of a cyber incident, this core capability includes efforts to coordinate activities across and among all levels of government and with private sector partners. This capability involves national operations centers, as well as on-scene response activities that manage and contribute to multi-agency efforts.

Planning

Description: Conduct a systematic process engaging the whole-of-Nation, as appropriate, in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.

In the context of a cyber incident, planning includes both deliberate planning and incident action planning. Deliberate planning involves developing strategic, operational, and tactical plans to prevent, protect against, mitigate the effects of, respond to, and recover from a cyber incident. Incident action planning occurs in a time-constrained environment to develop or rapidly adapt operational and tactical plans in response to an imminent or ongoing cyber incident.

Public Information and Warning

Description: Deliver coordinated, prompt, reliable, and actionable information to the whole-of-Nation and the public, as appropriate, through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threats or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.[33]

In the context of a significant cyber incident, this capability uses effective and accessible indications and warning systems to communicate significant cyber threats to involved or potentially involved operators, security officials, and the public (including alerts, detection capabilities, and other necessary and appropriate assets).

Screening, Search, and Detection

Description: Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence.

In the context of a cyber incident, this capability includes the measures which may be taken in response to actionable intelligence that indicates potential targets or types of malicious cyber activity, or the threat actors planning such activity. Measures may also be taken to verify or characterize a cyber threat that has already been located. Screening relative to a cyber incident may include monitoring the status of the network, assets, sensors, and other technologies that provide information on the security posture that may determine further action as necessary.

Situational Assessment

Description: Provide all decision makers with timely, decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response.

In the context of a cyber incident, this capability focuses on rapidly processing and communicating large quantities of information from across the broader community, from the field level to the national level, to provide all decision makers with the most current and accurate information possible.

Threats and Hazards Identification

Description: Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude of those threats; and incorporate this into analysis and planning processes

[33] The President of the United States has directed the Secretary of Homeland Security and the Attorney General to coordinate with each other to execute key responsibilities that provide public information and warning to the Nation regarding threats and incidents.

so as to clearly understand the needs of an entity.

In the context of a cyber incident, this capability involves the continual process of collecting timely and accurate data on cyber threats, including accounting for the future impacts of technology advancements, to meet the needs of analysts and decision makers. Effective Threats and Hazards Identification for a cyber incident is supported by standardized data sets, platforms, methodologies, terminologies, metrics, and reporting to unify levels of effort across all layers of government and the private sector, reducing redundancies.

Coordinating Structures and Integration

Successfully managing cyber incidents requires a whole-of-Nation approach (as described in the introduction of this document) that facilitates coordination among all stakeholders, including the private sector, SLTT governments, federal agencies, and international partners. Governing entities organize that coordination through established structures that promote unity of effort during incident response.

Coordinating structures provide a mechanism for representatives of entities that are affected by or are responsible for responding to a cyber incident to coordinate and facilitate response activities. These coordination and response activities may include preparedness activities, the delivery of capabilities, development operational plans, coordination of response personnel and activities, the crafting of unified public messaging and alerts, and weighing the technical, operational, political, and policy implications of varying courses of action.

While existing policies and coordinating structures can handle the vast majority of cyber incidents, significant cyber incidents may require a unique approach to coordinating the whole-of-Nation response. Pursuant to PPD-41, the U.S. Government will establish a Cyber UCG as the primary method for coordinating between and among federal agencies responding to a significant cyber incident, as well as for integrating SLTT governments and private sector partners into incident response efforts as appropriate for the specific incident. Other coordinating structures should be prepared to integrate and interoperate with a Cyber UCG, if one is established.

This section describes the major coordination structures in place across stakeholder communities that can be leveraged for response to cyber incidents requiring external coordination. Specifically, it describes how these structures will be leveraged, and additional structures incorporated, to provide operational coordination in response to significant cyber incidents.

Coordinating Structures

Stakeholders can utilize a variety of existing coordinating structures during any cyber incident to facilitate information sharing, coordinate response activities, access technical assistance and other resources, provide policy coordination and direction, and enable effective response. Most cyber incidents that occur on a daily basis are considered routine, and their responses are handled internally by the affected entity. As such, affected entities may choose to combine any of the coordinating structures below as deemed necessary to address the unique nature of the incident and specific organizational or sector needs. For significant cyber incidents, or cyber incidents that have implications for national security or public health and safety, PPD-41 establishes lead federal agencies and a coordinating structures framework with operational response planning and activities coordinated through a Cyber UCG.

Private Sector

For many years, the private sector has successfully engaged in coordination efforts between and across industry and government around detection, prevention, mitigation, and response to cyber incidents through information sharing, analysis, and collaboration. Each of the 16 critical infrastructure sectors and sub-sectors designated under PPD-21: *Critical Infrastructure Security and Resilience,*[34] has a self-organized and self-governed Sector Coordinating Council (SCC). SCC members include critical infrastructure owners and operators, industry trade associations, and others across the private sector. SCCs provide a forum for members to engage with others across their sector, companion Government Coordinating Councils (GCCs), and SSAs to collaboratively address the full range of sector-specific and cross-sector critical infrastructure security and resilience policy and strategy efforts.

In addition, the private sector critical infrastructure community has developed its own coordination efforts through established ISACs. ISACs are based in and organized and governed by the private sector (with the exception of the MS-ISAC discussed later), with operational capabilities that support the public-private partnership around critical infrastructure protection and cybersecurity every day. The National Council of ISACs routinely facilitates cross-sector coordination to further productive engagement across the private sector and with government at the federal, state, and local levels.

As mentioned earlier, in accordance with policy established by Executive Order 13691, DHS is facilitating efforts to identify procedures to create and accredit ISAOs[35] to allow groups of stakeholders to create information sharing groups based on affinity among members (e.g., geography, industry or community segment, or threat exposure) that could provide a more formalized structure for information sharing and the provision of technical assistance. Some organizations, including those that are well established and delivering value every day, may be recognized as an ISAO and or ISAC, or as a member of more than one, concurrently. ISACs predate and are a subset of ISAOs.

State, Local, Tribal, and Territorial Governments

These levels of government also have a variety of coordination structures available to them for cyber incident response. These structures support information sharing, incident response, operational coordination, and collaboration on policy initiatives among participating governments.

As with private sector organizations, SLTT governments can be members of ISACs, ISAOs, or other information sharing organizations. They could also be members of the SLTT GCC at the national policy coordination level. For incidents on SLTT government networks MS-ISAC provides information sharing and technical assistance to its members and has established relationships with the Federal Government. As owners and operators of critical infrastructure and key resources, certain SLTT government agencies could also be members of sector-specific ISACs and may also develop unique structures, tailored to their jurisdiction’s needs, to provide coordination and direction to response officials during a cyber incident. Many also collaborate with one another through selected cyber information sharing groups or organizations such as the National Association of State Chief Information Officers or the National Governors’ Association.

While many SLTT governments are developing and utilizing operational coordination structures for cyber incident response, they have not all adopted a standard approach. Some may designate their state or major urban area fusion center as the primary contact and information sharing hub for cyber incident coordination while others could leverage their respective emergency or security operations center. For cyber incidents with physical effects, or that have consequences that must be managed in collaboration with other emergency management agencies (e.g., fire departments, public health agencies, human services offices), emergency operations centers will also likely provide important

[34] https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[35] www.isao.org

information sharing and incident management functions. At the state/territory level, emergency operations centers often coordinate resource requests with federal agencies, including FEMA and DoD, and provide operational coordination with the National Guard. The SLTT community are encouraged to provide cross-functional training in cybersecurity for the employees of their emergency operations center. As appropriate, cyber incident responders should also receive emergency response and emergency operations center training.

Federal Government

The Federal Government organizes coordinating structures into three categories for cyber incident response:

- National policy level coordination through the Cyber Response Group (CRG),[36]
- Operational coordination through Federal Cybersecurity Centers and federal agencies, and
- Sector coordination through the SSAs and GCCs.

To coordinate policy at the National level, PPD-41 assigns the Assistant to the President for Homeland Security and Counterterrorism the responsibility to convene and chair the CRG to coordinate development and implementation of Federal Government policy and strategy with respect to significant cyber incidents affecting the Nation or its interests abroad. The CRG will coordinate the development and implementation of U.S. Government policy and strategy for responding to significant cyber incidents. Federal departments and agencies, including relevant cybersecurity centers, are invited to participate in the CRG, as appropriate, based on their respective roles, responsibilities, and expertise or in the circumstances of a given incident or grouping of incidents. Federal agencies, including SSAs that regularly participate in the CRG must establish and implement enhanced coordination procedures to manage significant cyber incidents that exceed their standing response capacities.

The Federal Government has established seven cybersecurity centers, with missions that include executing cyber operations, enhancing information sharing, maintaining situational awareness, and serving as conduits between public and private sector entities. Any or all of these centers should coordinate with federal entities and provide support to cyber incident response to the extent circumstances dictate and authorities permit. Pursuant to PPD-41, three of these centers coordinate significant cyber incident response activities within a Cyber UCG: the NCCIC, the NCIJTF, and CTIIC.

The Federal Government has also designated a number of SSAs to lead their sector GCCs, which are governmental counterparts to SCCs. SSAs are designated for each of the 16 critical infrastructure sectors designated under PPD-21. SSAs leverage their particular knowledge and expertise to fulfill a number of information sharing, coordination, incident response, and technical assistance responsibilities to their assigned critical infrastructure sector(s), as detailed in PPD-21 and the NIPP. GCCs include other government agencies with authorities and expertise in a given sector; robust engagement across GCC participants will enable interagency and interjurisdictional coordination by including broader participation from federal and SLTT governments, as appropriate to the needs of each sector.

[36] More information on the Cyber Response Group can be found within PPD-41: *U.S. Cyber Incident Coordination*. https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident; Annex for Presidential Policy Directive-41--United States Cyber Incident Coordination, https://www.whitehouse.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident.

International

International information sharing takes place through a variety of mechanisms in both the public and private sectors. Many organizations have information sharing relationships that extend to international partner companies and governments. International operational coordination can occur through relationships that federal departments and agencies have with their foreign counterparts and with international organizations, through formal diplomatic channels managed by DOS and through the relationships that private firms have internally, with other private sector entities, with national governments, and with international organizations.

Many federal agencies and cybersecurity centers have relationships with counterparts in foreign nations and routinely share information and collaborate, both during steady state and cyber incidents. Federal law enforcement agencies also maintain information sharing channels with foreign counterparts and the International Criminal Police Organization (INTERPOL) to facilitate international investigations. The FBI, through its Legal Attaché program, has designated Cyber liaison attaches stationed in U.S. Embassies. DHS/ICE HSI has broad legal authority to enforce a diverse array of federal statutes and uses this authority to investigate all types of cross-border criminal activity. The U.S. Secret Service maximizes partnerships with international law enforcement counterparts through overseas field offices and by forward deploying the Electronic Crimes Special Agent Program to international working groups. The NCCIC collaborates with international CSIRT partners to obtain situational awareness and determine priorities for protection and response. Organizations such as the DOS Overseas Security Advisory Council, for example, coordinates information sharing and collaborative security activity and analysis for U.S. private sector interests abroad through an industry representative council structure and established channels at U.S. embassies and other diplomatic posts. Additionally, some ISACs have chosen to open membership to firms and organizations located in friendly foreign nations, with safeguards in place to preserve confidentiality of information restricted to U.S. participants.

Given existing relationships and the overlapping policy and operational issues that may arise during a significant cyber incident, it is important to note that international coordination will likely occur through multiple channels concurrently.

Operational Coordination During a Significant Cyber Incident

Cyber incidents affect domestic stakeholders on an ongoing basis. The vast majority of these incidents pose no demonstrable risk to the U.S. national security interests, foreign relations, economy, public confidence, civil liberties, or public health and safety and thus do not rise to the designation of a significant cyber incident as defined by PPD-41 and the accompanying Cyber Incident Severity Schema in Annex B. Such cyber incidents are resolved either by the affected entity alone or with routine levels of support from, and in coordination with, other private sector stakeholders and/or from SLTT, federal, or international government agencies. In the event of a significant cyber incident, the Federal Government may form a Cyber UCG as the primary method for coordinating between and among federal agencies responding to a significant cyber incident and for integrating private sector partners into incident response efforts as appropriate.

Determination of Incident Severity

The Federal Government adopted the Cyber Incident Severity Schema in Annex B as a common framework and shared understanding to evaluate and assess cyber incidents at all federal departments and agencies when determining the severity of a cyber incident. Cyber incidents rated a “3” or greater will equate to a significant cyber incident. Federal Government departments and agencies shall leverage the Cyber Incident Severity Schema when assessing the severity level and the potential impact of cyber incidents to ensure common terminology, appropriate information sharing, and proper management to effectively address an incident. As referenced earlier, Annex C compares the Cyber Incident Severity Schema and Activation Level of the National Response Coordination Center to demonstrate alignment cyber and physical incidents. When assessing the severity of a potentially significant incident, the federal cybersecurity centers that serve as lead federal agencies under PPD-41 (the NCCIC, NCIJTF, and CTIIC) will consult to make a joint assessment of severity.

Our Nation's critical infrastructure sectors are composed of public and private owners and operators, both of which provide vital services and possess unique expertise and experience that the Federal Government and Nation rely heavily upon. Therefore, when determining incident severity, DHS, through the NCCIC and the SSAs of sectors affected or likely to be affected, may consult with sector leadership and private sector owners and operators through organizations such as the sector ISAC(s), SCC, GCC, the National Council of ISACs, MS-ISAC, and/or the Partnership for Critical Infrastructure Security if the incident affects or is likely to affect a non-federal entity in one or more of the critical infrastructure sectors. The private sector assessment would inform the NCCIC severity rating of a cyber incident.

With the majority of critical infrastructure owned and operated by the private sector, it is more than likely that the Federal Government may learn of a potential significant cyber incident through voluntary self-reporting and information sharing from the affected entity or a sector coordinating mechanism. Non-federal entities are also encouraged to utilize the Cyber Incident Severity Schema and/or the NCCIC Cyber Incident Scoring System[37] to help organizations provide a repeatable and consistent mechanism for estimating the risk of an incident.

Additionally, when a significant cyber incident affects a private sector stakeholder, SLTT government, or international counterpart, they have several options for voluntarily sharing the issue with federal authorities including:

- The NCCIC, FBI, or NCIJTF;
- Applicable SSA(s) or regulators; or
- The local field office of federal law enforcement agencies, including the FBI, U.S. Secret Service, U.S. ICE/HSI, or relevant Military Criminal Investigative Organizations if defense related.

Points of contact for reporting incidents to Federal Government entities are provided in Annex D: Reporting Cyber Incidents to the Federal Government. In addition to voluntary reporting, affected entities that have mandatory reporting requirements according to law, regulation, or contract must continue to comply with such obligations.

The federal agency that receives the report will coordinate with other federal agencies in responding to the incident, including determining whether or not to establish a Cyber UCG to coordinate the response to the significant cyber incident. As a part of this determination, stakeholders can provide information and assessments to federal agencies regarding their view of the severity of the incident for their entity and for their sector. Federal agencies will leverage these assessments and engage with the affected entity for discussion as part of the decision process. As appropriate, the Federal Government also engages with relevant private sector organizations, ISACs, ISAOs, SCCs, SLTT governments, and/or international stakeholders for consultation about the severity and scope of the incident.

[37] National Cyber Incident Scoring System. https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System.

Enhanced Coordination Procedures

Per PPD-41, each federal agency that regularly participates in the CRG, including SSAs, ensures that it has the standing capacity to execute its role in cyber incident response. Agencies establish enhanced coordination procedures to prepare for significant cyber incidents that exceed its standing capacity. These procedures require dedicated leadership, supporting personnel, available facilities (physical and communications), and internal processes enabling it to manage a significant cyber incident under demands that would exceed its capacity to coordinate under normal operating conditions.

Enhanced coordination procedures help to:

- Identify the appropriate pathways for communicating with other federal agencies during a significant cyber incident, including the relevant agency points-of-contact, and for notifying the CRG that enhanced coordination procedures were activated or initiated;
- Highlight internal communications and decision-making processes that are consistent with effective incident coordination; and
- Outline processes for maintaining these procedures.

In addition, each federal agency's enhanced coordination procedures identify the agency's processes and existing capabilities to coordinate cyber incident response activities in a manner consistent with PPD-41. Government and private sector personnel should obtain the necessary clearances and accesses to facilitate the quick sharing of information. PPD-41 also directs SSAs to develop or update sector-specific procedures, as needed and in consultation with the sector(s), for enhanced coordination to support response to a significant cyber incident, consistent with this directive. These sector-focused procedures serve as a key mechanism for integrating government and private sector response processes, including processes for accounting for and responding to the business impacts of significant incidents.

Cyber UCG

A Cyber UCG, per PPD-41, serves as the primary national operational coordination mechanism between and among federal agencies responsible for identifying and developing operational response plans and activities during a significant cyber incident, as well as for integrating private sector partners and the SLTT communities into incident response efforts, as appropriate.

Authorities

The Cyber UCG works to establish shared objectives for threat response, asset response, and intelligence support to guide cyber incident response and recovery efforts in the short to mid-term. PPD-41 establishes the Cyber UCG and frames this concept of operations. PPD-41 does not alter, supersede, or limit the authorities of federal agencies to carry out their functions and duties consistent with applicable legal authorities and other Presidential guidance and directives. Instead, PPD-41 complements and builds upon PPD-8 on National Preparedness by integrating cyber and traditional preparedness efforts to manage incidents that include both cyber and physical effects. It also leverages the SSA construct and assignments of PPD-21 on Critical Infrastructure Security and Resilience. The Cyber UCG bolsters a unity of effort and does not alter agency authorities or leadership, oversight, or command responsibilities, unless mutually agreed upon between the relevant agency heads and consistent with applicable legal authorities, including the Economy Act of 1932.

Cyber UCG Formation

A Cyber UCG will be formed and activated only in the event of a significant cyber incident and will be incident specific. Cyber UCG will be formed by any of the following processes:

- At the direction of the National Security Council Principals Committee (Secretary level), Deputies Committee (Deputy Security level), or the CRG;
- When two or more federal agencies that generally participate in the CRG, including relevant SSAs, request its formation based on their assessment of the cyber incident against the severity schema; and or
- When a significant cyber incident affects critical infrastructure owners and operators identified by the Secretary of Homeland Security for which a cyber incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security

A Cyber UCG will dissolve when enhanced coordination procedures for threat and asset response are no longer required or the authorities, capabilities, or resources of more than one federal agency are no longer required to manage the remaining facets of the federal response to an incident.

Cyber UCG Responsibilities

Per PPD-41, a Cyber UCG conducts the following activities to promote unity of effort in response to a significant cyber incident:

- Coordinates the cyber incident response in a manner consistent with the principles described in the Section III of PPD-41 Annex;
- Ensures all appropriate federal agencies, including SSAs, are incorporated into the incident response;
- Coordinates the development and execution of response and recovery tasks, priorities, and planning efforts, including international and cross-sector outreach, necessary to respond appropriately to the incident and to speed recovery;
- Facilitates the rapid and appropriate sharing of information and intelligence among Cyber UCG participants on the incident response and recovery activities;
- Coordinates consistent, accurate, and appropriate communications regarding the incident to affected parties and stakeholders (and those who could be affected), including the public as appropriate; and
- For incidents that include cyber and physical effects, forms a combined UCG with the lead federal agency or with any UCG established to manage the physical effects of the incident under the NRF developed pursuant to PPD-8: *National Preparedness*,[38] or other applicable presidential policy directives.

The Cyber UCG will promptly coordinate with DOJ, general counsel from DHS, regulators, and other relevant federal agencies' attorneys about pertinent legal issues as they are identified to quickly consider and coordinate them with appropriate nongovernmental entities, as necessary.

[38] PPD-8, *National Preparedness*, March 30, 2011. https://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf.

Cyber UCG Participation

Per PPD-41, when a Cyber UCG is established, the Federal Government establishes three lead agencies to effectively respond to significant cyber incidents:

- DHS is the lead agency for **asset response** during a significant cyber incident, acting through the NCCIC. The NCCIC includes representation from the private sector, SLTT, and numerous federal agencies. It is a focal point for sharing cybersecurity information, information about risks and incidents, analysis, and warnings among federal and non-federal entities.
- DOJ is the lead agency for **threat response** during a significant cyber incident, acting through the FBI and the NCIJTF. Consisting of over 20 partner agencies from across law enforcement, the IC, and the DoD, the NCIJTF serves as a multi-agency focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations.
- ODNI is the lead coordinator for **intelligence support** during a significant cyber incident, acting through the CTIIC. CTIIC provides situational awareness, sharing of relevant intelligence information, integrated analysis of threat trends, events, and support to interagency efforts to develop options to degrade or mitigate adversary threat capabilities. CTIIC also coordinates any intelligence collection activities that may take place as part of the incident, including identification of intelligence gaps, through the National Intelligence Manager, Cyber. Drawing upon the resources and capabilities across the Federal Government, the lead federal agencies are responsible for:
- Coordinating any multi-agency threat or asset response activities to provide unity of effort, to include coordinating with any agency providing support to the incident, to include SSAs in recognition of their unique expertise;
- Ensuring that their respective lines of effort are coordinated with other Cyber UCG participants and affected entities, as appropriate;
- Identifying and recommending to the CRG, if elevation is required, any additional Federal Government resources or actions necessary to appropriately respond to and recover from the incident; and
- Coordinating with affected entities on various aspects of threat, asset, and affected entity response activities through a Cyber UCG, as appropriate.

In addition to the lead federal agencies, a Cyber UCG will also include SSAs, if the cyber incident affects or is likely to affect sectors they represent as well as other federal cybersecurity centers as deemed necessary per the specific significant cyber incident. All federal agencies responding to the significant cyber incident will participate in, and coordinate their response activities with, a Cyber UCG.

SLTT government will be asked to participate in a Cyber UCG when the government entity owns or operates critical infrastructure that is or may be affected by that particular significant cyber incident. Otherwise, the Cyber UCG will use existing collaboration and information sharing mechanisms to provide regular updates to SLTT partners.

Like government participation, private sector involvement in a Cyber UCG will be limited to organizations with significant responsibility, jurisdiction, capability, or authority for response for that specific incident, which may not always include all organizations contributing resources to the response. Private Sector Cyber UCG participation will be voluntary and participants should be from organizations which can determine the incident priorities for each operational period and approve an Incident Action Plan, to include commitment of their organizations' resources to support execution of the Incident Action Plan. Per the Guiding Principles in PPD-41, out of respect for an affected entities' privacy and sensitive private sector information, the Federal Government will coordinate with the affected entity on the approach of wider incident dissemination for that incident. Cyber UCG participants will be expanded or contracted as the situation changes during that particular incident response.

Depending on the nature and extent of the incident, a Cyber UCG might also incorporate specific ICT[39] companies, also known as ICT enablers, to directly assist on that specific incident response. ICT enablers are companies whose functions and capabilities are the foundations of the global cyber ecosystem. As such, it is these ICT enablers who are often best positioned to share information, ensure engagement of key players across the Internet and ICT realms, and assist with large-scale response efforts during a significant cyber incident.

Additionally, the Cyber UCG will continue to use several pre-existing and well-established coordinating structures, such as SCCs, ISACs and routine operational calls, for information sharing to ensure appropriate and timely sharing of actionable intelligence. As the operational arm for many sectors, ISACs especially can assist in their specific sector and across sectors impact assessment as the specific incident allows. Additional organizations may be engaged in response as participants in a Cyber UCG staff or as liaising organizations working in cooperation with the incident management team under separate leadership structures. Such organizations would generally have awareness of and opportunities to provide input to the Incident Action Plan, but would not be responsible for its contents or execution.

Regardless of specific participant composition, a Cyber UCG shall operate in a manner that is consistent with the need to protect intelligence and law enforcement sources, methods, operations, and investigations, the privacy of individuals, and sensitive and protected private sector information.

Information Sharing During Cyber Incident Response

Cyber UCGs share cyber threat information developed during incident response with other stakeholders as quickly, openly, and regularly as possible, to ensure protective measures can be applied with all applicable stakeholders. This sharing may at times be constrained by law, regulation, interests of the affected entity, classification or security requirements, or other operational considerations. However, participants will strive for unity of message when sharing with stakeholders and the public. Existing cyber threat information sharing channels will be used to disseminate such information where feasible.

In some cases, depending on how a Cyber UCG's participants have decided to staff a particular incident, this sharing could also take place via a Public Information Officer designated by the Cyber UCG or via a Joint Information Center staffed by representatives of responding organizations. In some cases, ad hoc information sharing mechanisms are required to provide effective situational awareness to interested or affected stakeholders. In all cases, Cyber UCGs protect the privacy of individuals and sensitive private sector information, as appropriate.

Conclusion

America's efforts to strengthen the security and resilience of networked technologies are never finished. To achieve this security and resilience, the public-private partnership is integral to collectively identifying priorities, articulating clear goals, mitigating risk, and adapting and evolving based on feedback and the changing environment. The Federal Government, SLTT governments, and

[39] The President's National Security Telecommunications Advisory Committee's Information Technology Mobilization Scoping Report. May 21, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf

the Private and International partners remain resolute in its commitment to safeguard networks, systems and applications against the greatest cyber risks it faces, now and for decades to come.

The DHS Office of Cybersecurity and Communications will coordinate and oversee reviews and maintenance of the NCIRP in coordination with the DOJ, ODNI, and SSAs. The revision process includes developing or updating any documents necessary to carry out capabilities. Significant updates to the Plan will be vetted through a public-private senior-level review process. This Plan will be reviewed in order to accomplish the following:

- Assess and update information on the core capabilities in support of cyber and cyber-physical incident response goals and objectives.
- Ensure that it adequately reflects the organization of responsible entities.
- Ensure that it is compatible with doctrine and practices for the protection, prevention, mitigation, response, and recovery mission areas of the National Preparedness Goal.
- Update processes based on changes in the national threat/hazard environment.
- Incorporate lessons learned and effective practices from day-to-day operations, exercises, and actual incidents and alerts.
- Adapt to opportunities and challenges that arise as technology evolves and changes.
- Reflect progress in the Nation’s cyber incident response mission activities, the need to execute new laws, executive orders, and Presidential directives, as well as strategic changes to national priorities and guidance, critical tasks, or national capabilities.

Additions or updates to the NCIRP annexes may occur independently from reviews of the base document based on lessons learned from immediate statute or law changes, cyber exercises or real world incidents.

Annex A: Authorities and Statutes

The authorities listed below provide the legal basis for Federal Government threat response, asset response, and intelligence support activities. Other laws and regulations place additional requirements on certain critical infrastructure sectors.

This list is not exhaustive, but it can be leveraged as a foundational resource.

- Communications Act of 1934, Section 706 (Public Law [PL] 73-416)
- Cybersecurity Act of 2015 (PL 114 – 113)
- Defense Production Act of 1950 (PL 81-744), as amended
- Executive Order (EO) 12333: *United States Intelligence Activities*, as amended
- EO 12382: *President's National Security Telecommunications Advisory Committee, as amended*
- EO 12829: *National Industrial Security Program*, as amended
- EO 12968: *Access to Classified Information*, as amended
- EO 13549: *Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities*
- EO 13618: *Assignment of National Security and Emergency Preparedness Communications Functions*
- EO 13636: *Improving Critical Infrastructure Cybersecurity*
- EO 13691: *Promoting Private Sector Cybersecurity Information Sharing*
- Federal Information Security Modernization Act of 2014 (PL 113-283)
- Homeland Security Act of 2002 (as amended through Public Law 112-265)
- Homeland Security Presidential Directive (HSPD)-5: *Management of Domestic Incidents*
- Intelligence Authorization Act for Fiscal Year 2004 (PL 108-177)
- Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458)
- National Cybersecurity Protection Act of 2014 (PL 113-282)
- National Infrastructure Protection Plan of 2013, *Partnering for Critical Infrastructure Security and Resilience*
- National Security Act of 1947 (PL 80-253), as amended
- National Security Directive 42: *National Policy for the Security of National Security Telecommunications and Information Systems*
- National Security Presidential Directive-54/ HSPD-23: *Cybersecurity Policy*
- Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.
- Presidential Policy Directive (PPD)-8: *National Preparedness*
- PPD-21: *Critical Infrastructure Security and Resilience*
- PPD-25: *U.S. Policy on Reforming Multilateral Peace Operations*
- PPD-40: *National Continuity Policy*

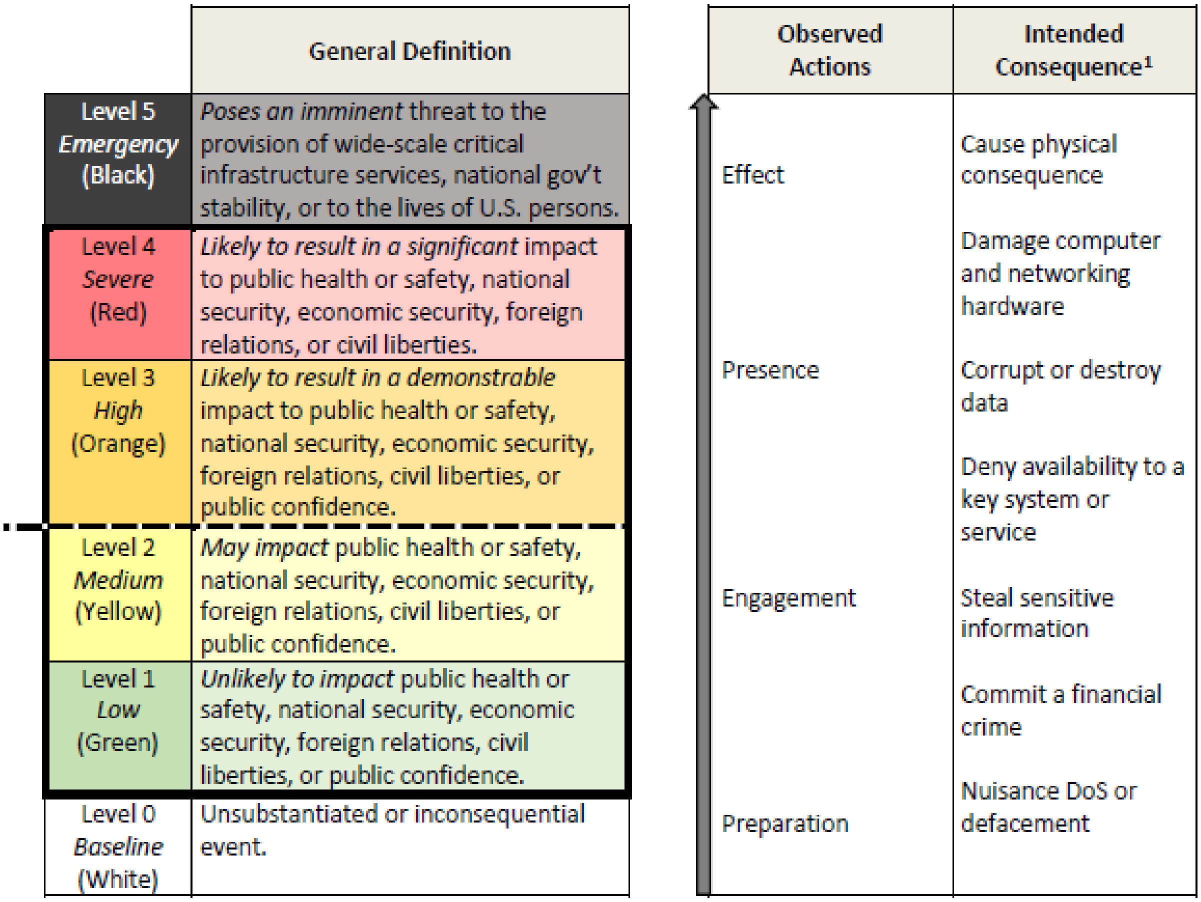
- PPD-41: *U.S. Cyber Incident Coordination Policy* and its accompanying Annex
- U.S. Code (USC) Title 6 – Domestic Security
- USC Title 10 – Armed Forces
- USC Title 18 – Crimes and Criminal Procedure
- USC Title 32 – National Guard
- USC Title 47 - Telecommunications
- USC Title 50 – War and National Defense

Annex B: Cyber Incident Severity Schema

Per Presidential Policy Directive (PPD)-41[40], the U.S. federal cybersecurity centers, in coordination with departments and agencies with a cybersecurity or cyber operations mission, adopted a common schema for describing the severity of cyber incidents affecting the homeland, U.S. capabilities, or U.S. interests. The schema establishes a common framework to evaluate and assess cyber incidents to ensure that all departments and agencies have a common view of the:

- Severity of a given incident;
- Urgency required for responding to a given incident;
- Seniority level necessary for coordinating response efforts; and
- Level of investment required for response efforts.

Figure 1 below depicts several key elements of the schema.



	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

Observed Actions	Intended Consequence[1]
Effect	Cause physical consequence
	Damage computer and networking hardware
Presence	Corrupt or destroy data
	Deny availability to a key system or service
Engagement	Steal sensitive information
	Commit a financial crime
Preparation	Nuisance DoS or defacement

Figure 1: Elements of the Cyber Incident Severity Schema

[40] https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber+Incident+Severity+Schema.pdf

Annex C: Cyber Incident Severity Schema/ National Response Coordination Center Activation Crosswalk

When incidents impact the cyber and/or physical environment(s), certain decisions and activities require coordination in order to respond in the most appropriate manner. The graphic below compares the Cyber Incident Severity Schema released in Presidential Policy Directive 41: United States Cyber Incident Coordination and the Department of Homeland Security National Response Coordination Center Activation Scale when comparing response levels for cyber and physical incidents.

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

Annex D: Reporting Cyber Incidents to the Federal Government[1]

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber incidents that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from Federal Government agencies, which are prepared to investigate the incident, help mitigate its consequences, and to help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims.

In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This Appendix explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government. A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

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

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal executive Branch civilian agencies to notify and consult with US-CERT regarding information security incidents involving their information and information systems, whether managed by a federal agency, contractor, or other source.

What to Report. A cyber incident may be reported at various stages, even when complete information is not available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

[1] This document was created in conjunction with Presidential Policy Directive 41 to provide the public with a unified federal message explaining how and when to report cyber incidents for purposes of obtaining assistance from the Federal Government. It does not address mandatory reporting pursuant to law, regulation, or contract. Such required reporting should continue to occur through designated federal points of contact using existing procedures.

How to Report Cyber Incidents to the Federal Government. Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, or any of the federal agencies listed in Table 1 below. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders to respond to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation, in addition to voluntarily reporting the incident to an appropriate federal point of contact. Federal agencies also collaborates with state, local, territorial and tribal government organizations as appropriate given the nature of the cyber incident.

Types of Federal Incident Response. Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: threat response and asset response:

- <u>Threat response</u> includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity.
- <u>Asset response</u> includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community and mitigating potential privacy risks to affected individuals.

Irrespective of the type of incident or its corresponding response, federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Table 1: Key Federal Points of Contact

Threat Response	Asset Response
Federal Bureau of Investigation (FBI): FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field Internet Crime Complaint Center (IC3): http://www.ic3.gov ▪ Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces. ▪ Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.	**National Cybersecurity and Communications Integration Center (NCCIC)** (888) 282-0870 or NCCIC@hq.dhs.gov **United States Computer Emergency Readiness Team:** http://www.us-cert.gov ▪ Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.
National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center: cywatch@ic.fbi.gov or (855) 292-3937 ▪ Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.	

Threat Response	Asset Response
United States Secret Service (USSS) Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): http://www.secretservice.gov/contact/field-offices ▪ Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.	
United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI) HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or www.ice.gov/webform/hsi-tip-form HSI Field Offices: https://www.ice.gov/contact/hsi HSI Cyber Crimes Center: https://www.ice.gov/cyber-crimes ▪ Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.	

If there is an immediate threat to public health or safety, the public should always call 911.

Annex E: Roles of Federal Cybersecurity Centers

The Federal Government has established a number of cybersecurity centers associated with various departments and agencies to execute operational missions, enhance information sharing, maintain situational awareness of cyber incidents, and serve as conduits between public-and private-sector stakeholder entities. In support of the Federal Government's coordinating structures on cyber incident management, a Cyber Unified Coordination Group[41] may elect to leverage these cybersecurity centers for their established enhanced coordination procedures, above-steady-state capacity, and/or operational or support personnel.

National Cybersecurity and Communications Integration Center (NCCIC)

As an operational element of the Department of Homeland Security, the NCCIC is the primary platform to coordinate the Federal Government's asset response to cyber incidents. The NCCIC is authorized under Section 3 of the National Cybersecurity Protection Act of 2014.

National Cyber Investigative Joint Task Force (NCIJTF)

The NCIJTF is a multi-agency center hosted by the Federal Bureau of Investigation and is the primary platform to coordinate the Federal Government's threat response. The NCIJTF is chartered under paragraph 31 of National Security Presidential Directive-54/Homeland Security Presidential Directive-23.

Cyber Threat Intelligence Integration Center (CTIIC)

Operated by the Office of the Director of National Intelligence, the CTIIC is the primary platform for intelligence integration, analysis, and supporting activities for the Federal Government. CTIIC also provides integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests.

U.S. Cyber Command (USCYBERCOM) Joint Operations Center (JOC)

The USCYBERCOM JOC directs the U.S. military's cyberspace operations and defense of the Department of Defense Information Network (DoDIN). USCYBERCOM manages both the threat and asset responses for the DoDIN during incidents affecting the DoDIN and receives support from the other centers, as needed.

National Security Agency Cybersecurity Threat Operations Center (NCTOC)

The National Security Agency Cybersecurity Threat Operations Center (NCTOC) is the 24/7/365 NSA element that characterizes and assesses foreign cybersecurity threats. The NCTOC informs partners of current and potential malicious cyber activity through its analysis of foreign intelligence, with a focus on adversary computer network attacks, capabilities, and exploitations. Upon request, the NCTOC also provides technical assistance to U.S. Government departments and agencies.

Department of Defense Cyber Crime Center (DC3)

DC3 supports the law enforcement, counterintelligence, information assurance, network defense, and critical infrastructure protection communities through digital forensics, focused threat analysis, and training. DC3 provides analytical and technical capabilities to federal agency mission partners conducting national cyber incident response.

[41] See page 30 for description.

Intelligence Community – Security Coordination Center (IC-SCC)

The IC-SCC mission is to monitor and oversee the integrated defense of the IC Information Environment in conjunction with IC mission partners and in accordance with the authority and direction of the Office of the Director of National Intelligence Chief Information Officer. The IC - Incident Response Center roles and responsibilities were assumed upon the IC SCC's founding in 2014.

Annex F: Core Capabilities and Critical Tasks

Each core capability identified in the National Cyber Incident Response Plan (NCIRP) has critical tasks that facilitate capability execution. These critical tasks are tasks that are essential to achieving the desired outcome of the capability. Critical tasks inform mission objectives, which allow planners to identify resourcing and sourcing requirements prior to an incident. The chart below describes each core capability and identifies critical tasks associated with each capability.

Core Capabilities and Critical Tasks
1. Access Control and Identity Verification **Description:** Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems. Also referred to as Authentication and Authorization.
Critical Tasks: • Verify identity to authorize, grant, or deny access to cyber assets, networks, applications, and systems that could be exploited to do harm. • Control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Perform audit activities to verify and validate security mechanisms are performing as intended. • Conduct training to ensure staff-wide adherence to access control authorizations.
2. Cybersecurity **Description:** Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorized use, and exploitation. More commonly referred to as computer network defense, these activities ensure the security, reliability, confidentiality, integrity, and availability of critical information, records, and communications systems and services through collaborative initiatives and efforts.
Critical Tasks: • Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited. • Secure, to the extent possible, public and private networks and critical infrastructure (e.g., communication, financial, electricity sub-sector, water, and transportation systems), based on vulnerability results from risk assessment, mitigation, and incident response capabilities. • Create resilient cyber systems that allow for the uninterrupted continuation of essential functions. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.

Core Capabilities and Critical Tasks

3. Forensics and Attribution

Description: Forensic investigations and efforts to provide attribution for an incident are complementary functions that often occur in parallel during a significant cyber incident.

Critical Tasks:

- Retrieve digital media and data network security and activity logs.
- Conduct digital evidence analysis, and respecting chain of custody rules.
- Conduct physical evidence collections, analysis adhere to rules of evidence collection as necessary.
- Assess capabilities of likely threat actors(s).
- Leverage the work of incident responders and technical attribution assets to identify malicious cyber actor(s).
- Interview witnesses, potential associates, and/or perpetrators if possible.
- Apply confidence levels to attribution assignments.
- Include suitable inclusion and limitation information for sharing products in attribution elements guidance.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Perform audit activities to verify and validate security mechanisms are performed as intended.

4. Infrastructure Systems

Description: Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity.

Critical Tasks:

- Maintain a comprehensive understanding of the needs for the safe operation of control systems.
- Stabilize and regain control of infrastructure.
- Increase network isolation to reduce the risk of a malicious cyber activity propagating more widely across the enterprise or among interconnected entities.
- Stabilize infrastructure within those entities that may be affected by cascading effects of the cyber incident.
- Facilitate the restoration and sustainment of essential services (public and private) to maintain community functionality.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Maintain up-to-date data knowledge of applicable emerging and existing security research, development, and solutions.

Core Capabilities and Critical Tasks

5. Intelligence and Information Sharing

Description: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as necessary.

Critical Tasks:

- Monitor, analyze, and assess the positive and negative impacts of changes in the operating environment as it pertains to cyber vulnerabilities and threats.
- Share analysis results through participation in the routine exchange of security information—including threat assessments, alerts, threat indications and warnings, and advisories—among partners.
- Confirm intelligence and information sharing requirements for cybersecurity stakeholders.
- Develop or identify and provide access to mechanisms and procedures for confidential intelligence and information sharing between the private sector and government cybersecurity partners.[42]
- Use intelligence processes to produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include critical infrastructure participants and partners with roles in physical response efforts.
- Share actionable cyber threat information with SLTT and international governments and private sectors to promote shared situational awareness.
- Enable collaboration via online networks that are accessible to all participants.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

[42] Information sharing must provide effective communication to individuals with access and functional needs, including people with limited English proficiency and people with disabilities, including people who are deaf or hard of hearing and people who are blind or have low vision. Effective communication with individuals with access and functional needs includes use of appropriate auxiliary aids and services, such as sign language and other interpreters, captioning of audio and video materials, user-accessible Web sites, communication in various languages, and use of culturally diverse media outlets.

Core Capabilities and Critical Tasks
6. <u>Interdiction and Disruption</u> **Description:** Delay, divert, intercept, halt, apprehend, or secure threats related to malicious cyber activity.
Critical Tasks: • Deter malicious cyber activity within the United States, its territories, and abroad. • Interdict persons associated with a potential cyber threat or act. • Deploy assets to interdict, deter, or disrupt cyber threats from reaching potential target(s). • Leverage law enforcement and intelligence assets to identify, track, investigate, and disrupt malicious actors threatening the security of the Nation's public and private information systems. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.
7. <u>Logistics and Supply Chain Management</u> **Description:** Facilitate and assist with delivery of essential commodities, equipment, and services to include the sustainment of responders in support of responses to systems and networks impacted by malicious cyber activity. Synchronize logistics capabilities and enable the restoration of impacted supply chains.
Critical Tasks: • Identify and catalog resources needed for response, prior to mobilization. • Mobilize and deliver governmental, nongovernmental, and private sector resources to stabilize the incident and integrate response and recovery efforts, to include moving and delivering resources and services to meet the needs of those impacted by a cyber incident. • Facilitate and assist delivery of critical infrastructure components to rapid response and restoration of cyber systems. • Enhance public and private resource and services support for impacted critical infrastructure entities. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Apply supply chain assurance principles and knowledge within all critical tasks identified above.

Core Capabilities and Critical Tasks

8. Operational Communications

Description: Ensure the capacity for timely communications in support of security, situational awareness, and operations, by any and all means available, among and between entities affected by the malicious cyber activity and all responders.

Critical Tasks:

- Ensure the capacity to communicate with both the cyber incident response community and the affected entity.
- Establish interoperable and redundant voice, data, and broader communications pathways between SLTT, particularly state fusion centers, federal, and private sector cyber incident responders.
- Facilitate establishment of quickly formed ad hoc voice and data networks on a local and regional basis so critical infrastructure entities can coordinate activities even if Internet services fail.
- Coordinate with any UCG (or entity) established to manage physical (or non-cyber) effects of an incident. Ensure availability of appropriate secure distributed and scalable incident response communication capabilities including out-of-band communications mechanisms where traditional communications and/or systems are compromised. Adhere to appropriate mechanisms for safeguarding sensitive and classified information private sector personnel should obtain the necessary clearances and accesses to facilitate the quick sharing of information.
- Protect individual privacy, civil rights, and civil liberties.
- Cyber threat information also is conducted through automated indicator sharing using established formats such as Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information (STIX/TAXII).[43]
- Perform red team activities to verify and validate that forensics and attribution capabilities are performing as intended and have adequate visibility.

9. Operational Coordination

Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrate all critical stakeholders and support execution of core capabilities.

Critical Tasks:

- Mobilize all critical resources and establish coordination structures as needed throughout the duration of an incident.
- Define and communicate clear roles and responsibilities relative to courses of action.
- Prioritize and synchronize actions to ensure unity of effort.
- Ensure clear lines and modes of communication between entities, both horizontally and vertically.
- Ensure appropriate private sector participation in operational coordination throughout the cyber incident response cycle consistent with the NIPP.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Perform table-top activities to verify and validate effective and appropriate coordination between stakeholders.

[43] https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

Core Capabilities and Critical Tasks

10. Planning

Description: Conduct a systematic process engaging the whole community, as appropriate, in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.

Critical Tasks:

- Initiate a flexible planning process that builds on existing plans as part of the National Planning System.[44]
- Collaborate with partners to develop plans and processes to facilitate coordinated incident response activities.
- Establish partnerships that coordinate information sharing between partners to restore critical infrastructure within single and across multiple jurisdictions and sectors.
- Inform risk management response priorities with critical infrastructure interdependency analysis.
- Identify and prioritize critical infrastructure and determine risk management priorities.
- Conduct cyber vulnerability assessments, perform vulnerability and consequence analyses, identify capability gaps, and coordinate protective measures on an ongoing basis in conjunction with the private and nonprofit sectors and local, regional/metropolitan, state, tribal, territorial, insular area, and federal organizations and agencies.
- Develop operational, business/service impact analysis, incident action, and incident support plans at the federal level and in the states and territories that adequately identify critical objectives based on the planning requirements; provide a complete and integrated picture of the escalation and de-escalation sequence and scope of the tasks to achieve the objectives; and are implementable within the time frame contemplated in the plan using available resources.
- Formalize partnerships such as memorandums of understanding or pre-negotiated contracts with governmental and private sector cyber incident or emergency response teams to accept, triage, and collaboratively respond to incidents in an efficient manner.
- Formalize partnerships between communities and disciplines responsible for cybersecurity and for physical systems dependent on cybersecurity. Formalize relationships such as memorandums of understanding or pre-negotiated contracts between information communications technology and information system vendors and their customers for ongoing product cyber security, business planning, and transition to response and recovery when necessary.
- Formalize partnerships with government and private sector entities for data and threat intelligence sharing, prior to, during, and after an incident.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

[44] The National Planning System provides a unified approach and common terminology to support the implementation of the National Preparedness System through plans that support an "all threats and hazards" approach to preparedness. These plans—whether strategic, operational, or tactical—enable the whole community to build, sustain, and deliver the core capabilities identified in the National Preparedness Goal.

Core Capabilities and Critical Tasks

11. <u>Public Information and Warning</u>

Description: Deliver coordinated, prompt, reliable, and actionable information to the whole community and the public, as appropriate, through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threat or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.

Critical Tasks:

- Establish accessible mechanisms and provide the full spectrum of support necessary for appropriate and ongoing information sharing among all levels of government, the private sector, faith-based organizations, nongovernmental organizations, and the public.
- Share actionable information and provide situational awareness with the public, private, and nonprofit sectors, and among all levels of government.
- Leverage all appropriate communication means, such as the Integrated Public Alert and Warning System, public media, and social media sites.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Respect applicable information sharing and privacy protections, including Traffic Light Protocol.
- Assure availability of redundant options to achieve critical public information, threat indication, and warning outcomes.

12. <u>Screening, Search, and Detection</u>

Description: Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence.

Critical Tasks:

- Locate persons and networks associated with cyber threats.
- Develop relationships and further engage with critical infrastructure participants (private industry and SLTT partners).
- Conduct physical and electronic searches as authorized by law
- Collect and analyze information provided.
- Detect and analyze malicious cyber activity and support mitigation activities.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.

Core Capabilities and Critical Tasks

13. Situational Assessment

Description: Provide all decision makers with decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response.

Critical Tasks:

- Coordinate the production and dissemination of modeling and effects analysis to inform immediate cyber incident response actions.
- Maintain standard reporting templates, information management systems, essential elements of information, and critical information requirements.
- Develop a common operational picture for relevant incident information shared by more than one organization.
- Coordinate the structured collection and intake of information from multiple sources for inclusion into the assessment processes.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

14. Threats and Hazards Identification

Description: Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of an entity.

Critical Tasks:

- Identify data requirements across stakeholders.
- Develop and/or gather required data in a timely and efficient manner to accurately identify cyber threats.
- Ensure that the right people receive the right data at the right time.
- Translate data into meaningful and actionable information through appropriate analysis and collection tools to aid in preparing the public.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Discover, evaluate and resolve gaps in policy, facilitate or enable technologies, partnerships, and procedures which are barriers to effective threat, vulnerability, and hazard identification for the sectors.

Annex G: Developing an Internal Cyber Incident Response Plan

This Annex describes processes that may be used for cyber incident response planning. The first subsection describes the national operational planning process. The second subsection outlines a planning process that individual entities may take.

National Operational Planning

An operational plan is a continuous, evolving instrument of anticipated actions that maximizes opportunities and guides response operations. Operational plans are "living documents," subject to revision as incidents evolve and new information becomes available. Operational plans seek to:

- Improve coordination, collaboration, and communication to identify and prioritize plans of actions and steps at various thresholds of escalation surrounding a cyber incident;
- Improve the ability to gather, analyze, and de-conflict multiple sources of information to produce timely and actionable situational awareness;
- Issue alerts and warnings across a broad range of stakeholders to raise awareness and initiate incident response activities, consequence management, and business continuity plans;
- Reduce redundancy and duplication that could adversely impact effective coordination by articulating and affirming various roles and responsibilities;
- Enhance predictability and sustainability to improve collaboration necessary to manage consequences and assess and mitigate impact; and
- Include flexibility and agility to adapt to emerging events and activities.

Operational planning is conducted across the broader community and is an inherent responsibility of every level of government and the private sector. Operational plans should be routinely exercised to ensure identify gaps and establish continuous improvement plans to improve preparedness and effectiveness of the information sharing process surrounding a cyber incident.

This NCIRP is not an operational plan for responding to cyber incidents. However, it should serve as the primary strategic approach for stakeholders to utilize when developing agency- and organization-specific operational plans. This common doctrine will foster unity of effort for emergency operations planning and it will help those affected by cyber incidents to understand how federal departments, agencies, and other national-level broader community partners provide resources to support the SLTT communities and private sector response operations.

Response Operational Planning

Both the Comprehensive Preparedness Guide (CPG) 101[45] and the Response Federal Interagency Operational Plan (FIOP) [46] are foundational documents that agencies and organizations can leverage and tailor to cyber incidents to develop their own operational response plans.

[45] CPG 101, Developing and Maintain Emergency Operations Plans, Version 2. November 2010. https://www.fema.gov/media-library/assets/documents/25975

[46] Response Federal Interagency Operational Plan, Second Edition. August 2016. https://www.fema.gov/media-library-data/1471452095112-507e23ad4d85449ff131c2b025743101/Response_FIOP_2nd.pdf

The CPG 101 provides information on various types of plans and guidance on the fundamentals of planning. Federal plans for incidents are developed using a six-step process, in alignment with the steps described in CPG 101:

- Form a collaborative planning team
- Understand the situation
- Determine the goals and objectives
- Develop the plan
- Prepare, review, and approve the plan
- Implement and maintain the plan.

The Response FIOP outlines how the Federal Government delivers the response core capabilities. The Response FIOP provides information regarding roles and responsibilities, identifies the critical tasks an entity takes in executing core capabilities, and identifies resourcing and sourcing requirements. It addresses interdependencies and integration with the other mission areas throughout the plan's concept of operations. It also describes the management of concurrent actions and coordination points with the areas of prevention, protection, mitigation, and recovery. It does not contain detailed descriptions of specific department or agency functions, as such information is located in department- or agency-level operational plans.

The NRF and NIMS guide the Response FIOP. The NRF is based on the concept of tiered response, with an understanding that most incidents start at the local and tribal level, and as needs exceed resources and capabilities, additional SLTT and federal assets are applied. The Response FIOP, therefore, aligns with other SLTT, insular area, and federal plans to ensure that all response partners share a common operational focus. Similarly, integration occurs at the federal level among the departments, agencies, and nongovernmental partners that compose the respective mission area through the frameworks, FIOPs, and departmental and agency operations plans.

Application

While the NRF does not direct the actions of other response elements, the guidance contained in the NRF and the Response FIOP informs SLTT and insular area governments, as well as nongovernment organizations and the private sector, regarding how the Federal Government responds to incidents. These partners can use this information to inform their planning and ensure that assumptions regarding federal assistance and response, and the manner in which federal support will be provided, are accurate.

Developing an Internal Cyber Incident Response Plan

Public and private sector entities should consider creating an entity-specific operational cyber incident response plan to further organize and coordinate their efforts in response to cyber incidents. Each organization should consider a plan that meets its unique requirements and relates to the organization's mission, size, structure, and functions.

The National Institute of Standards and Technology Special Publication 800-61 (revision 2)[47] outlines several elements to consider when developing a cyber incident response plan. Each plan should be tailored and prioritized to meet the needs of the organization and adhere to current information sharing and reporting requirements, guidelines, and procedures, where they exist. As

[47] NIST SP 800-61 Revision 2, Computer Incident Handling Guide. August 2012. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

appropriate, public and private sector entities are encouraged to collaborate in the development of cyber incident response plans to promote shared situational awareness, information sharing, and acknowledge sector, technical, and geographical interdependences.

The elements below serve as a starting point of important criteria to build upon for creating a cyber incident response plan:

- Mission
- Strategies and goals
- Organizational approach to incident response
- Risk assessments
- Cyber Incident Scoring System/Criteria[48]
- Incident reporting and handling requirements
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization
- Communications with outside parties, such as:
    - Customers, constituents, and media
    - Software and support vendors
    - Law enforcement agencies
    - Incident responders
    - Internet service providers
    - Critical infrastructure sector partners
- Roles and responsibilities (preparation, response, recovery)
    - State Fusion Center
    - Emergency Operations Center
    - Local, regional, state, tribal, and territorial government
    - Private sector
    - Private citizens
- A training and exercise plan for coordinating resources with the community
- Plan maintenance schedule/process.

[48] The NCCIC Cyber Incident Scoring System could be used as a basis for an organizations operations center to assist in the internal elevation of a particular incident. https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System.

Annex H: Core Capability/NIST Cybersecurity Framework/PPD-41 Crosswalk

The NCIRP Crosswalk describes the relationship between the NIST Cybersecurity Framework and PPD-41. By walking through the table below, each core capability is cross-referenced to ensure continuity and connection between the three documents. This table should be leveraged as a starting point that may assist in the NCIRP's response activities under each core capability, understanding the NIST's functions and categories, and the PPD's respective Lines of Effort.

NCIRP Core	Core Capability	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
Access Control	Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.		Access Control Protective Technology				Asset Response
Cybersecurity	Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorized use, and exploitation.	Asset Management Business Environment Risk Assessment Risk Management Strategy	Access Control Data Security Information Protection Processes and Procedures Protective Technology	Anomalies and Events Security Continuous Monitoring Detection Processes	Communications Response Planning Analysis Mitigation	Communications Improvements Recovery Planning	Asset Response
Forensics and	Forensic investigations and efforts to provide attribution for an incident are complimentary functions that often occur in parallel during a significant cyber incident.				Analysis		Threat Response Asset Response Intelligence Support

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
Infrastructure	Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity.	Asset Management Business Environment Risk Assessment	Access Control Data Security Information Protection Processes and Procedures Protective Technology	Anomalies and Events Security Continuous Monitoring Detection Processes		Communications Improvements Recovery Planning	Asset Response
Intelligence and Information Sharing	Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.	Asset Management Business Environment	Awareness & Training Data Security	Security Continuous Monitoring Detection Processes	Communications Analysis Mitigation Improvements	Communications	Threat Response Asset Response Intelligence Support
Interdiction and Disruption	Delay, divert, intercept, halt, apprehend, or secure threats						Threat Response

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
	related to malicious cyber activity.						
Logistics and Supply Chain Management	Facilitate and assist with delivery of essential commodities, equipment, and services to include the sustainment of responders in support of responses to systems and networks impacted by malicious cyber activity. Synchronize logistics capabilities and enable the restoration of impacted supply chains.	Business Environment					Asset Response
Operational Communications	Ensure the capacity for timely communications in support of security, situational awareness, and operations by any and all means available, among and between entities affected by the malicious cyber activity and all responders.	Asset Management		Communications	Communications		Threat Response Asset Response Intelligence Support
Operational Coordination	Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports execution of core capabilities.	Governance Risk Assessment Risk Management	Anomalies and Events				Threat Response Asset Response Intelligence Support
Planning	Conduct a systematic process engaging the whole community, as appropriate, in the development of executable strategic,				Response Planning	Recovery Planning Improvements	Threat Response Asset Response

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
	operational, and/or tactical-level approaches to meet defined objectives.						Intelligence Support
Public Information and Warning	Deliver coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threat or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.				Communications	Communications	Threat Response Asset Response Intelligence Support
Screening, Search and Detection	Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures.			Anomalies and Events Security Continuous Monitoring Detection Processes			Threat Response Asset Response Intelligence Support
Situational Assessment	Provide all decision makers with decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response. In the context of a cyber	Business Environment Communications Awareness and Training		Detection Processes	Communications	Communications	Threat Response Asset Response Intelligence Support

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
	incident, this capability focuses on rapidly processing and communicating large quantities of information from across the whole community from the field-level to the national-level to provide all decision makers with the most current and accurate information possible.						
Threats and Hazards Identification	Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of an entity.			Anomalies and Events Security Continuous Monitoring Detection Processes			Threat Response

Annex I: Additional Resources

The following resources can be leveraged by both the private and public sector. Entities can use this list as a starting point for understanding cyber incident response, vulnerability updates, data breach information, risk management, and organizations that serve as a points of contacts for the public and private sector. This non exhaustive alphabetical list provides a wide range of information that can also be leveraged beyond the scope of this document.

- Center for Internet Security: www.cisecurity.org
- CIS Critical Controls: https://www.cisecurity.org/critical-controls.cfm
- Cyber Incident Severity Schema: https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber+Incident+Severity+Schema.pdf
- DHS Critical Infrastructure Cyber Community Voluntary Program: https://www.us-cert.gov/ccubedvp
- Government Coordinating Councils: https://www.dhs.gov/gcc
- Information Sharing and Analysis Organizations: https://www.isao.org/
- Infragard: www.infragard.org
- Industrial Control System Security Computer Emergency Response Team: https://ics-cert.us-cert.gov
- Malware Investigator: https://www.malwareinvestigator.gov/
- MITRE Common Vulnerabilities and Exposures: https://cve.mitre.org/
- Multi-State Information Sharing and Analysis Center: https://msisac.cisecurity.org/
- National Council of Information Sharing and Analysis Centers: http://www.nationalisacs.org/
- National Incident Management System: https://www.fema.gov/national-incident-management-system
- National Vulnerability Database: https://nvd.nist.gov/
- NIST Framework for Improving Critical Infrastructure Cybersecurity: https://www.nist.gov/cyberframework
- NIST National Checklist Program Repository: https://web.nvd.nist.gov/view/ncp/repository
- NIST SP 800-61:: Revision 2: Computer Incident Handling Guide: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf:
- NIST SP 800-37: Guide to Applying the Risk Management Framework to Federal Information Systems: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
- NVD Common Vulnerability Scoring System: https://nvd.nist.gov/cvss.cfm Sector Coordinating Councils: https://www.dhs.gov/scc
- US-CERT Website: www.us-cert.gov

Annex J: Acronym List

CRG	Cyber Response Group
CTIIC	(Office of the Director of National Intelligence) Cyber Threat Intelligence Integration Center
DC3	Department of Defense Cyber Crime Center
DHS	Department of Homeland Security
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DoDIN	Department of Defense Information Network
DOJ	Department of Justice
DOS	Department of State
ESF	Emergency Support Functions
FBI	(Department of Justice) Federal Bureau of Investigations
FEMA	(Department of Homeland Security) Federal Emergency Management Agency
GCC	Government Coordinating Council
HSI	(Department of Homeland Security) Homeland Security Investigations
IC	Intelligence Community
IC3	Internet Crime Complaint Center
IC-SCC	Intelligence Community Security Coordination Center
ICE	(Department of Homeland Security) Immigrations and Customs Enforcement
ICT	Information and Communications Technology
INTERPOL	International Criminal Police Organization
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
JOC	Joint Operations Center
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCIRP	National Cyber Incident Response Plan
NCCIC	(Department of Homeland Security) National Cybersecurity and Communications Integration Center
NCIJTF	(Federal Bureau of Investigations) National Cyber Investigative Joint Task Force
NCPA	National Cybersecurity Protection Act
NCTOC	National Security Agency Cybersecurity Threat Operations Center
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology

NIPP	National Infrastructure Protection Plan
NRF	National Response Framework
ODNI	Office of the Director of National Intelligence
PII	Personally Identifiable Information
PPD	Presidential Policy Directive
SCC	Sector Coordinating Council
SLTT	State, Local, Tribal, and Territorial
SLTT GCC	State, Local, Tribal, and Territorial Government Coordinating Council
SSA	Sector Specific Agency
UCG	Unified Coordination Group
US-CERT	United States – Computer Emergency Readiness Team
USCYBERCOM	(Department of Defense) United States Cyber Command

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security

NATIONAL
SECURITY
ARCHIVE

National Security Archive,
Suite 701, Gelman Library, The George Washington University,
2130 H Street, NW, Washington, D.C., 20037,
Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu