DRAFT NATIONAL CYBER INCIDENT RESPONSE PLAN
SEPTEMBER 22, 2016

Attached for your review is the working draft of the National Cyber Incident Response Plan (NCIRP). The updated plan will formalize the incident response practices that have been developed over the past few years and will in further detail clarify organizational roles, responsibilities, and actions to prepare for, respond to, and coordinate the recovery from a significant cyber incident. This plan will build upon the Presidential Policy Directive (PPD-41) on U.S. Cyber Incident Coordination and include the private sector and other levels of government.

As part of a National Engagement Period, this draft of the NCIRP containing proposed updates is being widely distributed for review and feedback. This is a draft document and we feel it is important to seek your input at this critical juncture.

This update to the NCIRP focuses on discrete, critical content revisions. The proposed changes in the attached draft are the result of the public and private sector input to this point. While the focus of the NCIRP is on cyber incident response efforts, there is a broader architecture outlined within the National Preparedness System that establishes how the whole community prevents, protects against, mitigates, response to and recovers from all threats and hazards. The revisions also draw from lessons learned during the development of the Interim NCIRP, National Planning Frameworks, and Federal Interagency Operational Plans as well as large scale cyber exercises such as Cyber Storm series and the National Level Exercise 2012.

The feedback received supports the development of the second edition of the NCIRP for official government approval per PPD-41. Please distribute the draft to any applicable partners, stakeholder, or individuals.

We look forward to receiving your feedback and thank you for your continued contributions on this important endeavor.

V/R,
Department of Homeland Security

Table of Contents

[This page is left blank intentionally]

I. Introduction

The *National Cybersecurity Protection Act of 2014* (NCPA)[1] 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 41[2] (PPD-41) titled U.S. Cyber Incident Coordination, sets forth principles governing the Federal Government's response to any cyber incident, provides an architecture for coordinating the response to significant cyber incidents, and requires DHS to develop a National Cyber Incident Response Plan (NCIRP) 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 community approach to mitigating, responding to and recovering from a cyber incident. This whole-of-nation approach includes and strongly relies on public and private partnerships to address major cybersecurity risks to critical infrastructure.

- Response Plan Purpose and Organization –The purpose of the NCIRP is to provide 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 NCIRP is intended to be used by the Nation as well as enhance our international partners' understanding of the U.S. cyber incident coordination framework. This all-inclusive concept focuses efforts and enables the full range of stakeholders—individuals, the private and nonprofit sectors (including private and public owners and operators of infrastructure), state, local, tribal, territorial (SLTT), 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.

II. 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 establishing a successful incident response capability.

The NCIRP is the strategic framework for operational coordination among Federal and SLTT governments; the private sector; and with international partners. Developed according to the guiding principles outlined in PPD-41 and leveraging doctrine from the National Preparedness System and the National Incident Management System (NIMS),[3] the NCIRP sets the strategic

[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] Presidential Policy Directive 41: U.S. Cyber Incident Coordination. https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
[3] National Incident Management System. http://www.fema.gov/national-incident-management-system

framework for how the Nation plans, prepares for, and responds to cyber incidents by establishing an architecture for coordinating the broader whole community response during a significant cyber incident in accordance with U.S. law and policy. A comprehensive 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. [4]

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 to utilize when developing agency, sector, and organization-specific operational plans. Utilizing this common doctrine will foster unity of effort for emergency operations planning and 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. This Plan should serve as the basis for national cyber operational playbooks and individual critical infrastructure sector operational coordination plans as well as at the individual entity level. 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 of individuals 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 and 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 incident 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 efforts must be coordinated to achieve optimal results. Whichever Federal agency first becomes aware of a cyber incident will rapidly notify other relevant Federal agencies in order to facilitate a unified Federal response and ensure that the right

[4] 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

combination of agencies responds to a particular incident. When responding to a cyber incident in the private sector, unity of effort ensures that the overall Federal response is synchronized, which prevents gaps in service and duplicative efforts. SLTT governments also have responsibilities, authorities, capabilities, and resources that can be 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 U.S. 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) to describe the incident level and coordination to aid in determining the severity of an incident and the threshold for designation of a significant cyber incident.

Table 1: Cyber Incident Definitions from PPD-41

Incident	Definition
Cyber Incident	A cyber incident is defined as 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.

III. Relationship to National Planning Frameworks

While the focus of the NCIRP is on cyber incident response efforts, there is a broader architecture outlined within the National Preparedness System that establishes how the whole community prevents, protects against, mitigates, responds to and recovers from all threats and

hazards. Specifically, the National Response Framework (NRF)[5] sets the doctrine and provides guidance for how the Nation builds, sustains, and delivers the response core capabilities identified in the National Preparedness Goal.[6] 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 incident management structure for the NRF and NCIRP, 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 community 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 their authorities, management structures, communication capabilities and protocols, integrate with one another to achieve common goals. These concepts are essential to cyber incident response in that they address: (1) the development of a single set of incident objectives; (2) the use of a collective, strategic approach to incident management; (3) the improvement of information flow and coordination; (4) the creation of a common understanding of joint priorities and limitations; (5) the assurance that no agency's legal authorities are compromised or neglected; and (6) the optimization of the combined efforts of all participants in the incident.

The NRF also includes 14 Emergency Support Functions (ESF),[7] which are the Federal coordinating structures that group resources and capabilities into functional areas that are most frequently needed in a national response. ESFs have proven to be 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 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, is dependent upon the response activities needed to support the incident. Specifically, through ESF #2 (Communications), the Government can coordinate the response to and recovery from a 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 Section VI of this document will coordinate with the established ESFs, to include ESF#2.

The NRF describes the roles and responsibilities of the whole community and all partners involved within the Response mission area. Those response roles and responsibilities also apply to cyber incidents. Consistent with those roles and responsibilities, the next section describes the

[5] The National Response Framework is one of five frameworks in the National Preparedness System that 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

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

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

concurrent lines of effort and identifies key roles and responsibilities relevant within each line of effort for responding to a cyber incident.

IV. 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 D: Roles of Federal Cyber Centers. In responding to any cyber incident, Federal agencies shall undertake four concurrent lines of effort: threat response; asset response; intelligence and related activities; and the affected entity's internal response efforts (if applicable). For many cyber incidents, the Federal Government will not play a direct role in the affected entity's response efforts. Where possible, and especially where incidents involve critical infrastructure or may escalate on the Cyber Incident Severity Schema, the Federal Government will conduct outreach efforts with the affected entity and offer to assist with response activities, consistent with the guiding principles described in Section 2: Scope.

Concurrent Lines of Effort

Recognizing the shared responsibility for cybersecurity, response activities in the NCIRP are undertaken through four concurrent lines of effort: threat response, asset response, intelligence support and related activities, and the affected entity's response efforts.[8] 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 seek to facilitate their activities accordingly while responding to cyber incidents. Assessing potential risks to a sector or region, including potential cascading effects, developing courses of action to mitigate these risks, and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner are also critical asset response activities.

Threat and asset responders share some responsibilities and activities, which includes 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 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 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

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

response, and intelligence support. The Department of State (DOS) is responsible for representing U.S. 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, other Federal departments and agencies, including the DHS, the Department of Defense (DoD), and the Department of Justice (DOJ), maintain active 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 includes 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. 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 also falls within threat response activities. As described in the Concurrent Lines of Effort, threat responders and asset responders work together 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. Other Federal agencies such as DoD and Department of Energy may provide elements of threat response through their counterintelligence organizations, particularly when the incident involves their contractors and possible nation-state affiliated cyber actors.

A. Private Sector

Small, medium, and large private sector entities perform critical roles in supporting threat response activities by timely reporting and sharing of information regarding cyber incidents and malicious cyber activity, 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 C: 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 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 for enabling threat response activities.

B. State, Local, Tribal and Territorial Government

Many states have criminal statutes regarding unauthorized access or damage to computer systems, which may be implicated in a cyber incident. State law enforcement agencies have a critical role in investigating violations of these, and other statutes, related to malicious cyber activity, and coordinating with other law enforcement entities in conducting investigations that extend beyond their geographic or authoritative jurisdiction.

C. Federal Government

In response to cyber incidents, Federal law enforcement agencies work across SLTT, Federal, and international levels, and with private sector entities, to address both criminal and national security cyber threats. Federal law enforcement agencies, such as the Federal Bureau of Investigations (FBI), United States Secret Service (USSS), and Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), conduct threat response activities related to criminal activity involving their investigative jurisdictions, and conduct appropriate coordination.

DOJ's U.S. Attorneys Offices 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 is used to identify the source of cyber incidents and to gather pertinent cyber threat information. Nationwide coordination of cyber prosecutorial initiatives are conducted through the Computer Hacking and Intellectual Property for criminal matters and by the National Security Cyber Specialist Network for cyber threats to the national security. In addition, DOJ, through the FBI and the National Cyber Investigative Task Force (NCIJTF), shares investigative information and cyber threat intelligence, as appropriate, with other Federal agencies to aid in the analysis of cyber threats and vulnerabilities.

DHS law enforcement agencies, including the USSS and ICE-HSI, conduct threat response activities related to criminal activity involving their investigative jurisdictions.

When requested or directed, DoD may support threat response efforts for cyber incidents not involving the DoD Information Network (DoDIN). Support may be provided through DoD's U.S. Cyber Command's (USCYBERCOM) or other assets as appropriate such as identify cyber adversaries and when the situation warrants and is consistent with law and policy, pursue adversaries in cyberspace.

Pursuant to PPD-41, in the event of a significant cyber incident for which a Cyber Unified Coordination Group (UCG) is convened, the DOJ through the FBI and the 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 Section 6.2: Operational Coordination During a Significant Cyber Incident.

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 may also include 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 new intelligence and information through the appropriate channels; and facilitating information sharing and operational coordination with other Federal Government entities. 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 resources and capabilities in a timely, effective manner are also critical asset response activities.

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 and highlight the unity of effort and share responsibility necessary in protecting the nation against cyber incidents.

A. Private Citizens

Cyber incidents, in particular, 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. By implementing basic precautions, individuals can reduce the risk and potential impact of a cyber incident by keeping software patched and updated, avoiding suspicious websites and emails, and protecting their personal information and systems by utilizing strong password practices and multi-factor authentication.

B. Private Sector

The private sector, especially the owners and operators of critical infrastructure, play 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, are normally the first to identify an incident, and are often in the best place to respond to it. Private entities that have a mandatory reporting requirement should assure that they report incidents that meet the required reporting thresholds even if they may otherwise mitigate the event. 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. Similarly, private sector service providers provide technology services to a broad swath of private companies and government agencies and support incident response efforts for their customers based on the terms of established contacts.

Private sector cybersecurity practitioners and providers 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, 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 (SSAs) implementing the National Infrastructure Protection Plan (NIPP) [9] 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 need to provide information to other entities in the sector in order 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 law enforcement, counterintelligence activities as well as their respective sector Information Sharing Analysis Centers (ISACs) and other information sharing and analysis organizations.

However, cyber incidents, especially significant cyber incidents, may involve greater coordination with the Government, the SLTT community, 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, are called upon to support national-level incident response efforts in light of their capabilities. During such an event, the private sector often provides support or assistance to Federal departments and agencies on preparedness and response activities. Federal and SLTT regulators may also have mandatory reporting requirements for certain types of cyber incidents. 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 may 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 should share with government responders the information the standing services develop or pursue concerning a cyber incident. Private sector entity engagement of external experts for such purposes should include provisions for continuing access of the government responders to that information

C. State, Local, Tribal and Territorial Government

Ensuring the safety and welfare of citizens are fundamental responsibilities of government at every level. Toward these objectives, Chief Executives of each SLTT government are responsible for ensuring preparedness, response, and recovery activities within their jurisdiction. For cyber incidents, the standard emergency response roles and responsibilities may not be sufficient to address technical challenges. 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. In order to facilitate coordination during a significant cyber incident response operation, each Chief Executive should pre-designate a primary individual to serve as Senior Official to represent its government.

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

- Regional Homeland Security Offices and Fusion Centers;

[9] The National Infrastructure Protection Plan, 2013. https://www.dhs.gov/national-infrastructure-protection-plan

- Multi-State ISAC (MS-ISAC) that acts as a focal point for critical information exchange and coordination between the SLTT community and the Federal Government;
- DHS National Protection and Programs Directorate field personnel, including:
  - Supervisory, Regional, and District-level Cybersecurity Advisors (CSAs), 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 (PSAs), work closely with State Homeland Security Advisors as critical infrastructure protection specialists;
- The Governors Homeland Security Advisors Council provides a structure through which the 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 (SLTTGCC) 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 the 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, chief executives 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. Chief Executives 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.

D. Federal Government

Federal asset response to a cyber incident encompasses many resources and capabilities from across the Federal departments, agencies as well as with the private sector. In response to cyber incidents, the Federal Government works across the national, Federal, SLTT, international levels, and with private sector entities to assist in mitigation, recovery, and restoration activities.

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. Per the NCPA, DHS through the National Cybersecurity and Communications Integration Center (NCCIC) serves as the Federal civilian interface for the sharing of information related to cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities.[10] The NCCIC facilitates information sharing to help identify other entities at risk to the same or similar vulnerabilities, and shares mitigation

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

recommendations and best practices to protect those at risk. The NCCIC works in close coordination with representation from multiple agencies and the private sector, for sharing cybersecurity information, information about risks, and incidents, analysis, and warnings among Federal and non-Federal entities, and for facilitating coordination regarding cybersecurity risks and incidents across the Federal civilian and 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 incident coordination and response working with DHS and serving as a day-to-day Federal interface on prioritization and coordination of activities within their respective sector; 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 is responsible for ensuring consistent and integrated approaches across various critical infrastructure sectors and ensuring a nation-wide 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. SSAs receive support from the DHS NCCIC and National Infrastructure Coordinating Center (NICC) to maintain and provide situational awareness on threats, incidents, or events impacting critical infrastructure and facilitates 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.

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 counterparts and builds on regular information sharing and operational coordination relationships.

In some cases, regulatory or contract requirements may 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.

When incidents affect DoD assets, the DoD is responsible for asset response activities on the DoDIN, typically acting through USCYBERCOM and the DoD Cyber Crime Center (DC3). DoD provides advice on mitigation strategies and may play a role in the asset response to a significant cyber incident not involving the DoDIN through a Defense Support of Civil Authorities (DSCA) request initiated by DHS. The Defense Security Service on behalf of DoD provides cyber threat sharing, analysis, alerting, awareness, and assistance to the cleared contractors serving DoD as the SSA for the Defense Industrial Base.

When incidents affect intelligence community (IC) assets, the IC Security Coordination Center (IC SCC) is responsible for asset response. The Office of the Director of National Intelligence (ODNI) shall be responsible for managing the threat and asset response for the integrated defense

of the IC information environment through the IC Security Coordination Center, in conjunction with IC mission partners and with support from other Federal agencies, as appropriate.

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 Section 6.2: Operational Coordination during a Significant Cyber Incident.

Intelligence Support

Intelligence and related supporting activities play an important role to better understand the cyber incident and implemented 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; and share of related threat indicators; analysis of threats; identify and acknowledge gaps; and ultimately create a comprehensive picture of the incident.

A. Federal Government

ODNI, through the Cyber Threat Intelligence Integration Center (CTIIC), provides intelligence support in response to cyber incidents. In this role, the CTIIC coordinates development of Federal intelligence information for the other Federal cyber centers and Federal stakeholders. This support may include 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. The CTIIC also coordinates any intelligence collection activities that may take place as part of the incident.

The DHS Office of Intelligence and Analysis has responsibilities under Title 6[11] to provide analysis and warnings related to threats against and vulnerabilities to certain non-Federal stakeholders and works through the NCCIC to share cyber-related intelligence and threat information during cyber incidents.

The FBI coordinates the sharing of relevant intelligence and information between both 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.

The 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,

[11]United States Code, 2012 Edition, Supplement 3, Title 6 – Domestic Security. Subchapter II – Information Analysis and Infrastructure Protection, Part A -Access to Information Sec. 124a - Homeland security information sharing. https://www.gpo.gov/fdsys/pkg/USCODE-2015-title6/pdf/USCODE-2015-title6-chap1-subchapII-partA-sec124a.pdf

capabilities, and exploitations. Upon request, the NCTOC also provides technical assistance to U.S. Government departments and agencies.

The IC may identify classified information indicating a potential credible cyber threat to an SLTT, critical infrastructure owner/operator, or other private sector entity. The Defense Security Service may provide this notification for cleared contractors in collaboration or coordination with DHS and/or the FBI. In accordance with Section 4 of Executive Order 13636, DHS and/or the FBI provides appropriate notification to the targeted entity. 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 other factors of national security concern exist, incident response processes and procedures adhere to all guidelines and directions for handling matters of national security.

Pursuant to PPD-41, in the event of a significant cyber incident for which a Cyber Unified Coordination Group (UCG) is convened, ODNI through the 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 Section 6.2: Operational Coordination during a Significant Cyber Incident.

Affected Entity's Response

Entities affected by a 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 may include maintaining business or operational continuity; mitigate potential health and safety impacts; addressing adverse financial impacts; protection of 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 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 (PII), then the appropriate Senior Agency Officials for Privacy will be notified and lead any necessary PII incident response process as required by the Office of Management and Budget Memorandum M-07-1612, Safeguarding Against and Responding to the Breach of PII (and its subsequent revisions), and the agency's Breach

Response Plan.[12], Safeguarding Against and Responding to the Breach of PII, and the agency's Breach Response Plan.

V. Core Capabilities

Core capabilities are the distinct critical elements needed to conduct the three lines of effort–threat response, asset response, and intelligence support–for 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 describing the significant functions that must be developed and executed across the whole community to ensure preparedness. 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 capabilities described in this section align to the National Preparedness Goal core capabilities. While in the National Preparedness Goal, the core capabilities are organized into mission areas, this section provides an explanation of *what* each capability entails and the context in which the nation must be prepared to execute it according to the three lines of effort previously mentioned – threat response, asset response, and intelligence support.

While some of the core capabilities are specific to one line of effort, many span across all three. For example, incident response planning is the inherent responsibility of all levels of government and private sector entities, especially the owners and operators of critical infrastructure, regardless of whether they are engaged in threat response, asset response, or intelligence support activities. Interdependencies also exist and many core capabilities are linked to one another through shared assets and services. For example, threat response activities such as interdiction of a threat actor and providing attribution could lead to important information sharing and operational synchronization with asset response and intelligence support activities.

This section is not intended to be an exhaustive list of capabilities, but rather a description of the capabilities that should be developed and utilized appropriate to 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.

Responding to a cyber incident, like incident response for all other threats and hazards, is a shared responsibility. The whole community must work together to ensure the U.S. is optimally prepared for cyber incidents; yet not every network/system faces the same risks.

SSAs should develop and update their Sector-Specific Plans to establish goals and priorities for the sector that address their current risk environment, such as the nexus between cyber and physical security, interdependence between various sectors, risks associated with climate change, aging and outdated infrastructure, and the need to ensure continuity in a workforce that is rapidly approaching retirement. By applying the actions outlined in the plans, sector participants should

[12] 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

be able to create products and tools that support the local and regional jurisdictions where facilities and systems are located and events take place.

By engaging the whole community to build and deliver the 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. The core capabilities are grouped in Table 2 by cross-cutting capabilities, threat response and asset response lines of effort.

Table 2: Core Capabilities by Line of Effort

Threat Response	Asset Response	Intelligence Support
Forensics and Attribution		
Intelligence and Information Sharing		
Operational Communications		
Operational Coordination		
Planning		
Public Information and Warning		
Screening, Search and Detection		
Interdiction and Disruption **Threats and Hazards Identification**	**Access Control and Identify Verification** **Cybersecurity** **Infrastructure Systems** **Logistics and Supply Chain Management** **Situational Assessment**	

1. Cross-Cutting Core Capabilities

Six response core capabilities—Intelligence and Information Sharing, Operational Communications, Operational Coordination, Planning, Public Information and Warning, and Screening, Search, and Detection—span across all three lines of effort outlined in PPD-41. These common core capabilities are essential to the success of the other core capabilities. They help establish unity of effort among all those involved in responding to the cyber incident.

A. Forensics and Attribution

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

i. Forensics:

Forensics is the term applied to the discovery and identification of information relevant to an investigation through the use of both scientific and intelligence-base 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 for the purpose of uncovering artifacts relevant to identifying malicious cyber activity. Forensics includes several sub-disciplines including: host-based forensics, network and packet data forensics, 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 how an adversary conducted a specific attack and how to defend against these or similar attacks. 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 may vary depending on the entities' varied access to particularized datasets or holdings.

ii. Attribution:

Attribution is the identification of an adversary linked to a particular event. It is the culmination of the review of evidence and intelligence gathered during an incident which contributes to an assessment that a particular individual, organization, or nation-state may have played a role in the cyber incident.

Attribution occurs over the life-cycle of an investigation and is not often determined at the onset of threat, asset or intelligence response. Although the development of attribution for a significant cyber event 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 may also be significant to an affected entity as it considers whether to pursue additional legal or civil action against an attacker.

Critical Tasks:

- Retrieve digital media and data network security and activity logs.

- Conduct digital evidence analysis respecting chain of custody rules where applicable.
- Conduct physical evidence collections and 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 made as appropriate.
- Inform attribution elements guidance with suitable inclusion and limitation information for sharing products.
- Adhere to appropriate mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

This capability also includes unique and technical capabilities that support computer network and asset analysis during an incident. Each of these supporting activities aim to provide awareness that paints a comprehensive picture to ultimately help reduce the impact of a current incident and prevent future cyber incidents from spreading across the network. These are described in greater detail in Annex G: Best Practices/Recommended Ongoing Activities.

B. 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 U.S.

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 intelligence and information sharing between the private sector and government cybersecurity partners.[13]
- 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 the SLTT and international government, and private sectors to promote shared situational awareness.
- Enable collaboration via on-line networks that are accessible to all participants.
- Adhere to appropriate mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

C. 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 the identification of 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, the focus of this capability is 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.

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 local, state, tribal, territorial, private sector, and Federal cyber incident responders.
- Facilitate establishment of hastily 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.
- Adhere to appropriate mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

[13] 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 and user-accessible Web sites, communication in various languages, and use of culturally diverse media outlets.

D. **Operational Coordination**

Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports execution of core capabilities. This is the capability to conduct actions and activities that enable senior decision makers across the whole community 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, ensures coordination of 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 the Annex C: Reporting Cyber Incidents to the Federal Government.

In the context of cyber incident, this 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.

Critical Tasks:

- Mobilize all critical resources, 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.
- Assure appropriate private sector participation in operational coordination throughout the cyber incident response cycle consistent with the NIPP.
- Adhere to appropriate mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

E. **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.

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.

Critical Tasks:

- Initiate a flexible planning process that builds on existing plans as part of the National Planning System.[14]
- Collaborate with partners to develop plans and processes to facilitate coordinated incident response activities.
- Establish partnerships that facilitate coordinated information sharing between partners to support the restoration of critical infrastructure within single and across multiple jurisdictions and sectors.
- Assure risk management-informed response priorities are appropriately informed by critical infrastructure interdependency analysis.
- Identify and prioritize critical infrastructure and determine risk management priorities.
- Conduct cyber vulnerability assessments, perform risk 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, 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 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 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.
- Adhere to appropriate mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

F. Public Information and Warning

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.

In the context of a cyber incident, this capability uses effective and accessible indications and warning systems to communicate significant cyber threats to involved or potentially involved

[14] 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.

operators, security officials, and the public (including alerts, detection capabilities, and other necessary and appropriate assets).[15]

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, non-government organizations, and the public.
- Promptly share actionable information and provide situational awareness with the private sector, public sector and among all levels of government, and nonprofit sector.
- Leverage all appropriate communication means, such as the Integrated Public Alert and Warning System, public media, social media sites, and technology.
- Adhere to appropriate 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, indication and warning outcomes.

G. 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 type of malicious cyber activity, or the threat actors planning such attacks. 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.

Critical Tasks:

- Locate persons and networks associated with cyber threat.
- Develop relationships and further engage with critical infrastructure participants (private industry and SLTT partners).
- Conduct authorized physical and electronic searches.
- Collect and analyze information provided.
- Detect and analyze malicious cyber activity and support mitigation activities.
- Adhere to appropriate 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.

[15] Public Information and Warning systems must provide effective communication to individuals with disabilities, such as audio and video captioning for multimedia and use-accessible Web sites. Public Information and Warning should also be communicated using various languages and culturally diverse media outlets.

2. Threat Response Core Capabilities

A. 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 or programs, or equipment/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 that violate the law.

Critical Tasks:

- Deter malicious cyber activity within the United States, its territories, and abroad.
- Interdict persons associated with a potential cyber threat or act.
- Strategically 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 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.

B. 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.

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.

Critical Tasks:

- Identify data requirements across stakeholders.
- Develop and/or gather required data in a timely and efficient manner in order to accurately identify cyber threats.
- Ensure that the right data are received by the right people 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 mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Evaluate and enable resolution of gaps in policy, facilitating or enabling technologies, partnerships and procedures which are barriers to effective threat, vulnerability and hazard identification for the sectors.

3. Asset Response Core Capabilities

A. 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.

This capability relies on the implementation and maintenance of protocols to verify identity and authorize, grant, or deny cyber access to specific information and networks.

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 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.

B. 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, power grid, 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 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.

C. Forensics and Attribution

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

i. Forensics:

Forensics is the term applied to the discovery and identification of information relevant to an investigation through the use of both scientific and intelligence-base 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 for the purpose of uncovering artifacts relevant to identifying malicious cyber activity. Forensics includes several sub-disciplines including: host-based forensics, network and packet data forensics, 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 how an adversary conducted a specific attack and how to defend against these or similar attacks. 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 may vary depending on the entities' varied access to particularized datasets or holdings.

ii. Attribution:

Attribution is the identification of an adversary linked to a particular event. It is the culmination of the review of evidence and intelligence gathered during an incident which contributes to an assessment that a particular individual, organization, or nation-state may have played a role in the cyber incident.

Attribution occurs over the life-cycle of an investigation and is not often determined at the onset of threat, asset or intelligence response. Although the development of attribution for a significant cyber event 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 may also be significant to an affected entity as it considers whether to pursue additional legal or civil action against an attacker.

Critical Tasks:

- Retrieve digital media and data network security and activity logs.
- Conduct digital evidence analysis respecting chain of custody rules where applicable.
- Conduct physical evidence collections and 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 made as appropriate.
- Inform attribution elements guidance with suitable inclusion and limitation information for sharing products.
- Adhere to appropriate mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

This capability also includes unique and technical capabilities that support computer network and asset analysis during an incident. Each of these supporting activities aim to provide awareness that paints a comprehensive picture to ultimately help reduce the impact of a current incident and prevent future cyber incidents from spreading across the network. These are described in greater detail in Annex G: Best Practices/Recommended Ongoing Activities.

D. 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.

Critical Tasks:

- Deep understanding of the needs for the safe operation of control systems.
- Stabilize and regain control of infrastructure.
- Increase network isolation to reduce risk of cyber-attack 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 mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Maintain up to date data knowledge of mitigation applicable emerging and existing security research and development, and solutions.

E. Logistics and Supply Chain Management

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.

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.

Critical Tasks:

- Mobilize and deliver governmental, nongovernmental, and private sector resources to stabilize the incident and facilitate the integration of 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 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.

F. 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. In the context of a cyber 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.

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 mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

4. Intelligence Support Core Capabilities

The core capabilities – Forensics and Attribution, Intelligence and Information Sharing, Operational Communications, Operational Coordination, Planning, Public Information and Warning, and Screening, Search, and Detection – for the intelligence support line of effort are included under the 'Cross-Cutting Core Capabilities' sub-section.

VI. Coordinating Structures and Integration

Successfully managing cyber incidents requires a whole-of-nation approach that facilitates coordination among all stakeholders including the private sector; SLTT governments; Federal agencies; and international partners. That coordination is organized through established structures that promote unity of effort during incident response. Coordinating structures are entities comprised of representatives from multiple departments, agencies, or private sector organizations applicable to the incident responsible for facilitating the preparedness and delivery of capabilities, developing operational plans, coordinating response personnel and activities, crafting unified public messaging and alerts, and weighing the political and policy implications of varying courses of action.

While the vast majority of cyber incidents can be handled through existing policies and coordinating structures, 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 private sector partners into incident response efforts as appropriate. Other coordinating structures should be prepared to integrate and interoperate with a Cyber UCG, should one be established.

The purpose of this section is to describe 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.

1. Coordinating Structures

There are a variety of existing coordinating structures stakeholders can utilize 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 handled internally by the affected entity. As such, affected entities may choose to utilize any combination 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.

A. 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 events through information sharing, analysis, and collaboration. This has most notably been accomplished across the private sector critical infrastructure community through established ISACs. ISACs are sector based and private sector organized and governed, with operational capabilities that support the public – private partnership around critical infrastructure protection and cybersecurity every day. Cross sector coordination is facilitated routinely through the

National Council of ISACs in furtherance of productive engagement across the private sector and with government at the Federal, state, and local level.

In addition, each of the designated 16 critical infrastructure sectors and sub-sectors designated under PPD-21 (*Critical Infrastructure Security and Resilience*) [16] 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. SCC's 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.

Further, in accordance with policy established by Executive Order 13691, DHS is facilitating efforts to identify procedures for creating and accrediting Information Sharing and Analysis Organizations (ISAOs) to allow for 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, or a member of more than one ISAO and/or ISAC concurrently.

B. State, Local, Tribal, and Territorial

SLTT governments 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 may also be members of the SLTTGCC at the national policy coordination level. In day to day operations coordination, many SLTT governments are members of the MS-ISAC, which 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 may also be members of sector-specific ISACs. SLTT governments 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 Governor's Association.

While many SLTT governments are developing and utilizing operational coordination structures for cyber incident response, there is no standard approach adopted by all SLTT governments. Most are still likely to designate their state or major urban area fusion center as the primary contact and information sharing hub for cyber incident coordination. Most of the states have at least one Fusion Center, which provides a mechanism for SLTT governments to share homeland security information and analysis with one another and with the Federal Government, including classified information. However, not all Fusion Centers have commensurate cyber incident response capabilities. For cyber incidents with physical effects, or that have consequences that

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

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 serve important information sharing and incident management functions. At the state/territory-level, emergency operations centers are often used to coordinate resource requests with Federal agencies, including FEMA and DoD, and to provide operational coordination with the National Guard.

C. 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), operational coordination through Federal Cyber Centers and Federal agencies, and sector coordination through the SSAs and GCCs.

To coordinate policy at the National level, PPD-41 assigns the National Security Council (NSC) the responsibility to convene and chair the CRG to coordinate development and implementation of U.S. Government policy and strategy with respect to significant cyber incidents affecting the nation or its interests abroad. Federal departments and agencies, including relevant cyber centers, shall be 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 and SSAs that regularly participate in the CRG shall develop and implement enhanced coordination procedures and mechanisms for significant cyber incidents that exceed their capacity to respond.

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 may 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 have been assigned responsibility to coordinate significant cyber incident response activities within a Cyber UCG; these are the NCCIC, the NCIJTF, and the CTIIC.

The Federal Government has also designated a number of SSAs who 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 enable interagency and inter-jurisdictional coordination and include members from Federal and SLTT governments, as appropriate to the needs of each sector.

D. 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. 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.

Many Federal Cyber Centers have formal and informal relationships with their 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. Additionally, 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.

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.

2. Operational Coordination During a Significant Cyber Incident

Cyber incidents affect domestic stakeholders on an ongoing basis. The majority of these incidents do not pose a 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 as for integrating private sector partners into incident response efforts as appropriate.

A. Determination of Incident Severity

The Federal Cybersecurity Centers adopted the Cyber Incident Severity Schema established under PPD-41 as a common framework for evaluating and assessing cyber incidents at all Federal departments and agencies to promote a shared understanding when determining the severity of a cyber incident. Incidents rated a "3" or greater will equate to a significant cyber incident. Federal Government departments and agencies should leverage the Cyber Incident Severity Schema when assessing the severity level and the potential impact of cyber incidents to ensure common terminology, sharing information, and proper management to effectively address an incident.

Our Nation's critical infrastructure sectors are comprised 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, SCC, the National Council of ISACs, 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 will 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 the Federal Government will 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[17] 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 or SLTT government, international counterparts, or they have assistance they can provide, they have several options for voluntarily sharing the issue with Federal authorities. They have the option of contacting any of the following Federal organizations:

- The NCCIC or NCIJTF,
- Applicable SSA(s),
- The local field office of Federal law enforcement agencies, including the FBI, USSS, or U.S. ICE/HSI, or relevant Military Criminal Investigative Organizations if defense related,
- The local DHS PSA or CSA.

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 this report will coordinate with other Federal agencies in responding to the incident, including determining whether or not to establish a Cyber UCG to coordinate response to significant cyber incidents. 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 would also engage with relevant private sector organizations, ISACs, ISAOs, SCCs, SLTT governments, and/or International stakeholders for consultation about the severity and scope of the incident.

B. Enhanced Coordination Procedures

Per PPD-41, each Federal agency that regularly participates in the CRG, including SSAs, shall ensure that it has the standing capacity to execute its role in cyber incident response. To prepare for situations in which the demands of a significant cyber incident exceed its standing capacity agency's will establish enhanced coordination procedures. 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.

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

Enhanced coordination procedures help 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 shall identify the agency's processes and existing capabilities to coordinate cyber incident response activities in a manner consistent with PPD-41.

C. Cyber UCG

A Cyber UCG, per PPD-41, will serve 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 determined using the Cyber Incident Severity Schema as well as for integrating private sector partners and the SLTT Community into incident response efforts, as appropriate. The Cyber UCG is intended to bolster a unity of effort and not to 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.

Per PPD-41, a Cyber UCG will be formed under any of the following processes:

- At the direction of the NSC 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,
- When a significant cyber incident affects critical infrastructure owners and operators identified by the Secretary of Homeland Security as owning or operating critical infrastructure for which a cyber incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

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

- Coordinate the cyber incident response in a manner consistent with the principles described in the PPD-41 Annex;
- Ensure all appropriate Federal agencies, including SSAs, are incorporated into the incident response;
- Coordinate 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;
- Facilitate the rapid and appropriate sharing of information and intelligence among Cyber UCG participants on the incident response and recovery activities;
- Coordinate 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, form 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[18] on National Preparedness or other applicable presidential policy directives.

The Cyber UCG will promptly coordinate with general counsel from DOJ, DHS, and other relevant Federal agencies attorneys about pertinent legal issues as they are identified to ensure they are quickly considered and coordinated with appropriate non-governmental entities, as necessary.

A Cyber UCG shall 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.

D. Structure of a Cyber UCG

The Cyber UCG and coordinate their response activities with the Cyber UCG. Per PPD-41, when a decision is made to establish a Cyber UCG, the Federal Government establishes three lead agencies to effectively respond to significant cyber incidents:

- The lead agency for asset response during a significant cyber incident is DHS, 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.
- The lead agency for threat response during a significant cyber incident is the DOJ, acting through the FBI and the NCIJTF. Comprised 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.
- The lead coordinator for intelligence support during a significant cyber incident is ODNI, acting through the CTIIC. The CTIIC provides situational awareness, sharing of relevant intelligence information, integrated analysis of threat trends, events, identification of knowledge gaps, and the ability to degrade or mitigate adversary threat capabilities.

Drawing upon the resources and capabilities across the Federal Government, the Federal lead 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

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

- Coordinating with affected entities on various aspects of threat, asset, and affected entity response activities through a Cyber UCG, as appropriate.

A Cyber UCG will also include SSAs, if a cyber incident affects or is likely to affect sectors they represent. In addition, as required by the scope, nature, and facts of a particular significant cyber incident, a Cyber UCG may include participation from other Federal agencies, SLTT governments, nongovernmental organizations, international counterparts, or the private sector. Each Chief Executive should pre-designate a primary individual to serve as Senior Official to represent its organization.

Participation in a Cyber UCG will be limited to organizations with significant responsibility, jurisdiction, capability, or authority for response, which may not always include all organizations contributing resources to the response. Cyber UCG 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. All Federal agencies responding to the significant cyber incident shall participate in a Cyber UCG and coordinate their response activities with the Cyber UCG.

Depending on the nature and extent of the incident, a Cyber UCG might also incorporate specific ICT[19] 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. Cyber UCG participants may be expanded or contracted as the situation changes during that particular incident response.

Additionally, several pre-existing and well-established coordinating structures for information sharing will continue to be utilized by the Cyber UCG to ensure appropriate and timely sharing of actionable intelligence. 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, all Cyber UCG participants shall safeguard the privacy of individuals, sensitive government information and proprietary private sector information, as appropriate.

[19] 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/Final%20NSTAC%20Information%20Technology%20Mobilization%20Scoping%20Report.pdf

E. Information Sharing During Cyber Incident Response

To the maximum extent allowed by applicable law, Cyber UCGs will 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, the 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 members have decided to staff a particular incident, this sharing may 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 may be required in order to provide effective situational awareness to interested or affected stakeholders. In all cases, a Cyber UCG shall operate in a manner that is consistent with the need to protect the privacy of individuals and sensitive private sector information, as appropriate.

VII. 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 in order to produce timely and actionable situational awareness;
- Issue alerts & warning 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 may adversely impact effective coordination by articulating and affirming various roles and responsibilities;
- Enhance predictability and sustainability to improve collaboration necessary to manage consequences, assess and mitigate impact; and
- Including flexibility and agility to adapt to emerging events and activities.

Operational planning is conducted across the whole community and is an inherent responsibility of every level of government and the private sector, especially owners and operators of critical infrastructure. 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. Utilizing this common doctrine will foster unity of effort for emergency operations planning and will help those affected by cyber incidents understand

how Federal departments and agencies and other national-level whole community partners provide resources to support the SLTT Community and private sector response operations.

Response Operational Planning

Both the Comprehensive Preparedness Guide (CPG) 101 and the Response Federal Interagency Operational Plans (FIOPs) are foundational documents that can be leveraged and tailored to cyber incidents by agencies and organizations developing their own operational response plans. 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.[20] These steps are:

- Form a collaborative planning team
- Understand the situation
- Determine the goals and objectives
- Plan development
- Plan preparation, review, and approval
- Plan implementation and maintenance

The Response FIOP outlines how the Federal Government delivers the response core capabilities.[21] 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, is intended to align with other SLTT, insular area government, 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 is intended to inform SLTT and insular area governments, as well as non-government organizations and the private sector, regarding how the Federal Government responds to incidents. These partners can use this information to inform their

[20] For more information regarding the Comprehensive Planning Guide 101, please see: https://www.fema.gov/media-library/assets/documents/25975.

[21] For more information regarding the Response Federal Interagency Operational Plan, please see: http://www.fema.gov/Federal-interagency-operational-plans.

planning and ensure that assumptions regarding Federal assistance and response and the manner in which Federal support will be provided are accurate.

VIII. Conclusion

America's efforts to strengthen the security and resilience of networked technologies is never finished. To achieve this security and resilience, the public-private partnership is integral to collectively coming together and identifying priorities, articulating clear goals, mitigating risk, and adapting and evolving based on feedback and the changing environment. The Federal Government remains resolute in its commitment to safeguard networks, systems and applications against the greatest cyber risks it faces, now and for decades to come. This means that this Response Plan is a living document and regular reviews of this Plan will ensure consistency with existing and new policies, evolving conditions, and the NPS and NIMS.

Annex A: Authorities and Statutes

The authorities listed below serve as a reference to the vast landscape of legislation the Federal Government operates in while also depicting the converging environments of technology, security, and intelligence into *threat response, asset response, and intelligence support* activities while also recognizing sector-specific regulations that provide additions requirements. While this lists Federal authorities it is recognized certain critical infrastructure sectors are under various sector regulations as outlined by law. While this list is not exhaustive it can be leveraged as a foundational resource.

- Presidential Policy Directive (PPD) 41: U.S. Cyber Incident Coordination Policy
- Cybersecurity Act of 2015, (P.L. 114 – 113)
- National Cybersecurity Protection Act of 2014, (P.L. 113-282)
- Federal Information Security Modernization Act of 2014
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity
- PPD-21: Critical Infrastructure Security and Resilience
- PPD-8: *National Preparedness*
- Executive Order (EO) 12333: *United States Intelligence Activities*, as amended
- National Security Presidential Directive (NSPD)-54/ Homeland Security Presidential Directive (HSPD)-23: *Cybersecurity Policy*
- NSPD-51/HSPD-20: *National Continuity Policy*
- Office of Management and Budget Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information. Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458, 118 Stat. 3638)
- Intelligence Authorization Act for Fiscal Year 2004 (Public Act 108-177)
- HSPD-5: *Management of Domestic Incidents*
- Title II, Homeland Security Act (Title II, Public Law 107-296)
- National Infrastructure Protection Plan 2013, Partnering for Critical Infrastructure Security and Resilience
- National Security Directive 42: *National Policy for the Security of National Security Telecommunications and Information Systems*
- 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 13691: Promoting Private Sector Cybersecurity Information Sharing
- EO 12472: *Assignment of National Security and Emergency Preparedness Telecommunications Functions*
- EO 12382: *President's National Security Telecommunications Advisory Committee*
- Defense Production Act of 1950, as amended
- National Security Act of 1947, as amended
- Section 706, Communications Act of 1934, as amended (47 U.S.C. 606)
- United States Code: Title 6 – Domestic Security
- United States Code: Title 10 – Armed Forces
- United States Code: Title 18 – Crimes and Criminal Procedure
- United States Code: Title 28, Section 0.85(a) – Criminal Justice Policy Coordination
- United States Code: Title 32 – National Guard
- United States Code: Title 47 - Telecommunications

- United States Code: Title 50 – War and National Defense

In addition, several key Federal decisions may be made to trigger additional Federal authorities. These decisions include—

- Declaration of a major disaster or emergency under the Stafford Act, Section 501 B (Pre-Eminent Federal Responsibility), as appropriate
- As appropriate, request support from the Defense Support of Civil Authorities (DSCA), or request technical assistance from an element of the U.S. Intelligence Community pursuant to EO 12333
- Use of the Economy Act
- Economic Espionage Act
- Insurrection Act
- National Emergencies Act
- Declaration of a public health emergency as warranted based on the severity of the cascading effects of the cyber incident(s)
- Request for the invocation of mutual assistance agreements, as appropriate
- Issuance of a Declaration of Emergency or Extraordinary Declaration of Emergency to facilitate resources, access specific funds, or quarantine or seize animals or products as a result of the cascading effects of a cyber incident
- Determination of whether the incident is an act of terrorism or an intentional criminal act.

Annex B: Cyber Incident Severity Schema

Per Presidential Policy Directive-41, 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 for evaluating and assessing cyber incidents to ensure that all departments and agencies have a common view of the:

- The severity of a given incident;
- The urgency required for responding to a given incident;
- The seniority level necessary for coordinating response efforts; and
- The level of investment required of response efforts.

The table below depicts several key elements of the schema.

	General Definition	Observed Actions	Intended Consequence[1]
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.	Effect	Cause physical consequence
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.		Damage computer and networking hardware
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.	Presence	Corrupt or destroy data
			Deny availability to a key system or service
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Engagement	Steal sensitive information
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.		Commit a financial crime
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.	Preparation	Nuisance DoS or defacement

Annex C: Reporting Cyber Incidents to the Federal Government

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 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 fact sheet 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.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be 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.

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, and any of the Federal agencies listed in the table on page two. The Federal agency receiving the initial report will coordinate with other relevant Federal stakeholders in responding 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.

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. Threat response 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. Asset response 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>
<tr><th colspan="2">Key Federal Points of Contact</th></tr>
<tr><th>Threat Response</th><th>Asset Response</th></tr>
<tr><td>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.</td><td rowspan="2">National Cybersecurity and Communications Integration Center (NCCIC)

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.</td></tr>
<tr><td>National Cyber Investigative Joint Task Force

(NCIJTF) CyWatch 24/7 Command Center:
(855) 292-3937 or cywatch@ic.fbi.gov

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.</td></tr>
</table>

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 https://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 D: Roles of Federal Centers

The Federal Government has established a number of cyber centers associated with various departments and agencies in order to execute operational mission, 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 may elect to leverage these cyber 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 serves as 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 serves as 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 will serve as the primary platform for intelligence integration, analysis, and supporting activities. 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. USCYBERCOM's National Mission Forces may play a role in the response to a significant cyber incident not involving the DoDIN through a Defense Support of Civil Authorities (DSCA) request.

National Security Agency/Central Security Service Threat Operations Center (NTOC)

The National Security Agency/Central Security Service (NSA/CSS) 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.

Defense Cyber Crime Center (DC3)

Operating under the Air Force Inspector General, 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.

Intelligence Community - Security Coordination Center (IC-SCC)

The IC SCC is one of the National Cybersecurity Centers and its mission is to monitor and oversee the integrated defense of the IC Information Environment (IC IE) in conjunction with IC mission partners in accordance with the authority and direction of the Office of the Director of National Intelligence (ODNI), Chief Information Officer (IC CIO). The Intelligence Community Incident Response Center (IC-IRC) roles and responsibilities were assumed upon the IC SCC's founding in 2014.

Annex E: Types of Cyber Incident/Attack Vectors

External/Removable Media - An attack executed from removable media or a peripheral device— for example, malicious code spreading onto a system from an infected Universal Serial Bus flash drive.

Attrition - An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a Distributed Denial of Service intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, or digital signatures).

Web - An attack executed from a website or web - based application — for example, a cross – site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.

Email – An attack executed via an email message or attachment – for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.

Impersonation – An attack involving replacement of something benign with something malicious – for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks involve impersonation.

Improper Usage – Any incident resulting from violation of an organization's acceptable usage policies by an unauthorized user – for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.

Loss or Theft of Equipment – The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token.

Other – An attack that does not fit into any of the other categories.

Annex F: Developing an Internal Cyber Incident Response Plan

Public sector 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, which relates to the organization's mission, size, structure, and functions.

The National Institute of Standards and Technology Special Publication 800-61 (revision 2) 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, adhere to current information sharing and reporting requirements, guidelines, and procedures, where they exist. The elements below serve as a starting point of important criteria to build upon for creating a cyber incident response plan. As appropriate, public sector 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.

- Mission
- Strategies and goals
- Organizational approach to incident response
- Risk Assessments
- Cyber Incident Scoring System/Criteria [22]
- 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 may include:
    - 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 Centers
    - Emergency Operations Center
    - Regional SLTT
    - Private sector
    - Private citizens
- A training and exercise plan for coordinating resources with the community
- Plan maintenance schedule/process

[22] 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 G: Federal Policy Coordination Mechanism

Cyber Response Group

At the national policy coordination level, per Presidential Policy Directive-41 (PPD-41), the Cyber Response Group (CRG), in support of the National Security Council (NSC) Deputies and Principals Committees, and accountable through the Assistant to the President for Homeland Security and Counterterrorism (APHSCT) to the NSC chaired by the President, shall coordinate the development and implementation of U.S. Government policy and strategy with respect to significant cyber incidents affecting the U.S. or its interests abroad.

Per the Annex to PPD-41, it shall:

- Coordinate the development and implementation of the Federal Government's policies, strategies, and procedures for responding to significant cyber incidents;
- Receive regular updates from the Federal cybersecurity centers and agencies on significant cyber incidents and measures being taken to resolve or respond to those incidents, including those involving personally identifiable information (PII);
- Resolve issues elevated to it by subordinate bodies as may be established, such as a Cyber UCG;
- Collaborate with the Counterterrorism Security Group and Domestic Resilience Group when a cross-disciplinary response to a significant cyber incident is required;
- Identify and consider options for responding to significant cyber incidents, including those involving PII, and make recommendations to the Deputies Committee (Deputy Secretary level), where higher-level guidance is required, in accordance with PPD-1 on Organization of the NSC System of February 13, 2009, or any successor; and
- Consider the policy implications for public messaging in response to significant cyber incidents and coordinate a communications strategy, as necessary, regarding a significant cyber incident.

The CRG shall be chaired by the Special Assistant to the President and Cybersecurity Coordinator (Chair), or an equivalent successor, and shall convene on a regular basis and as needed at the request of the APHSCT and Deputy National Security Advisor. Federal departments and agencies, including relevant cyber centers, shall be 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.

CRG participants shall generally include senior representatives from the Departments of State, the Treasury, Defense (DoD), Justice (DOJ), Commerce, Energy, Homeland Security (DHS) and its National Protection and Programs Directorate, and the United States Secret Service, the Joint Chiefs of Staff, Office of the Director of National Intelligence, the Federal Bureau of Investigation, the National Cyber Investigative Joint Task Force, the Central Intelligence Agency, and the National Security Agency. The Federal Communications Commission shall be invited to participate should the Chair assess that its inclusion is warranted by the circumstances and to the extent the Commission determines such participation is consistent with its statutory authority and legal obligations.

Annex H: Crosswalk - NIST Cybersecurity Framework and NCIRP Core Capabilities

Annex I: Best Practices or Recommended Ongoing Activities

By engaging the whole community to build and deliver the cyber incident response core capabilities, the Nation is better prepared to respond to any cyber threat, assist in restoring basic services and community functionality, and facilitate the integration of recovery activities. Incident Response is just one aspect of cybersecurity, but it spans multiple mission areas. The best practices below describe critical tasks that small, medium, and large organizations and individuals should be aware of that is outside the scope of incident response, but is also important in safeguarding networks and assets. These best practices are also meant to complement existing security measures that are relative to cybersecurity in general.

1. Long-Term Vulnerability Reduction

Description: Build and sustain resilient systems, communities, critical infrastructure, and key resources lifelines so as to reduce their vulnerability to malicious cyber activity by lessening the likelihood, severity, and duration of the adverse consequences.
In the context of a cyber incident, this capability focuses on taking stock of current and emerging cyber threats; assessing the current risk and ability to recover from malicious cyber activity; developing a plan that addresses identified vulnerabilities; and analyzes available resources, processes, programs, and funding opportunities. The result is informed action that leads to lasting reductions in vulnerability to cyber networks and systems.

Critical Tasks:

- Work to shape the cyber ecosystem. This ranges from our work to encourage companies to build security into their software and hardware systems in the first place, to our work to stimulate the insurance industry to address cyber security risks, to our work to increase the number of our nation's cybersecurity professionals.
- Supporting security researchers and encouraging responsible disclosure etiquette and norms and laws that support prompt patching of vulnerabilities.
- Strongly encourage cyber best practices throughout the private sector, amongst all Federal, and state, local, tribal, and territorial actors, to include individual citizens and international partners.

2. Risk and Disaster Resilience Assessment

Description: Assess risk and disaster resilience relating to malicious cyber activity so that decision makers, responders, and community members can take informed action to reduce their entity's risk and increase their resilience.

In the context of a cyber incident, this capability is the evaluation of the cyber threat, vulnerability, consequences, needs, and resources through formal, standardized methods to define and prioritize risks, so critical infrastructure participants, decision makers, and responders can make informed decisions and take the appropriate action. Such an assessment directly connects cyber threat and impact data in order to analyze and understand the potential effects on an asset, a critical infrastructure sector, and/or a community.

3. Risk Management for Protection Programs and Activities

Description: Identify, assess, and prioritize risks of malicious cyber activity to inform risk mitigation activities, countermeasures, and investments.

In the context of a cyber incident, this capability includes implementing and maintaining risk assessment processes to identify and prioritize cyber assets, systems, networks, and functions, as well as implementing and maintaining appropriate tools to identify and assess threats, vulnerabilities, and consequences.

Critical Tasks:

- Gather required data in a timely and accurate manner to effectively identify risks.
- Develop and use appropriate tools to identify and assess cyber threats, vulnerabilities, and consequences.
- Leverage risk-informed standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts.
- Identify, implement, and monitor risk management plans.
- Validate, calibrate, and enhance risk assessments by relying on experience, lessons learned, and knowledge beyond raw data or models.
- Use risk assessments to design exercises and determine the feasibility of mitigation projects and initiatives.

4. Supply Chain Integrity and Security

Description: Strengthen the security and resilience of the supply chain.
Protecting the cyber supply chain relies on a layered, risk-based, proactive, and balanced approach in which security measures and resiliency planning are integrated into supply chains. In the context of a cyber incident, this capability relies ensuring the integrity, availability, and confidentiality of information, key nodes, methods of transport between nodes, and materials in transit between a cyber supplier and an owner/operator of the critical cyber network or system.

While long-term supply chain security and resiliency efforts are required, validation of the security of the supply chain may be required when responding to a complex cyber incident. Even with effective supply chain resiliency planning, the expansive nature of the global supply chain renders it vulnerable to disruption from intentional or naturally occurring causes. This capability employs real-time verification and detection, flexibility, and redundancy to ensure the availability for goods and services during a cyber incident, and requires a broad efforts from stakeholders across international and domestic public and private sectors.

Critical Tasks:

- Verify and detect malicious or counterfeit components or systems.
- Deploy physical protections, countermeasures, and policies to secure and make resilient key cyber nodes, methods of transport between nodes, and materials in transit during incident response efforts.
- Execute secure supply chain management to preempt supply chain disrupting during incident response, to identify items of concern during incident response, and to prevent the distribution of malicious or counterfeit hardware and software.
- Develop redundancies and mitigation measures in real-time for key dependencies and interdependencies related to supply chain operations.
- Notify government and private sector stakeholders impacted by cyber incidents of supply chain risks.

5. Technical Capabilities

The following technical capability activities could also be leveraged in core capabilities such as the Forensics and Attribution as well as Intelligence and Information Sharing. These technical capabilities demonstrate that information and intelligence may be shared to serve different purposes for each stakeholder.

a. Host System Forensic Analysis

Description: Host system forensic analysis is a methodology where an analyst conducts a deep dive of a single system or asset. The intent of this analysis is to identify the initial compromise or adversary presence, determine what actions were taken on the system and/or what elements of the system were changed. Special attention is paid to how an adversary first enters a system and how this system was used to access other systems or resources on the network. Additional host system forensics focuses on what information is accessed and/or retrieved by the actor. This information is often presented in a timeline format so it can be correlated with other events during a response of a single system or asset.

Critical Tasks:

- Memory Analysis
- Network Connection Analysis
- Time-lining
- File System Triage Analysis

b. Cyber Event Correlation

Description: Cyber event correlation is a capability for an analyst to correlate timeline and log data to create a comprehensive view of adversary activity during a response. In most cases, behavioral analysis and baselining will be used to identify anomalous activity that may appear non-malicious, but out of place, on first inspection. Special attention is paid to how an adversary moves from one system to other systems and what avenues of exploitation were used. Cyber event correlation typically uses log files and events from a variety of sources, including physical security sources.

Critical Tasks:

- Log aggregation
- Time-lining including physical security correlation when indicated
- User behavior profiling

c. Network and Packet Analysis

Description: Network and packet analysis is a capability set for analysts to analyze network traffic patterns, anomalies, and protocols at a deep level. This capability may start with simple anomaly detection using network flow or other telemetry data. Analysts will also conduct manual or automated reviews of packet content and protocol usage to identify anomalous and potentially malicious behavior.

Critical Tasks:

- Protocol specific knowledge
- Network traffic analysis

- Anomaly detection
- Baselining

d. Malicious Code Analysis

Description: Malicious Code analysis is the skill set for conducing the reverse engineering and analysis of malicious or potentially malicious code artifacts. Malicious Code Analysts are trained in static and dynamic code analysis, malware reverse engineering, anti-anti-forensics techniques, code de-obfuscation, and machine languages (for multiple processor sets).

Critical Tasks:

- Dynamic code analysis
- Static code analysis
- Anti-anti-forensics techniques
- Assembly/Machine language interpretation (multiple processor sets)
- Cryptography
- Packet analysis
- Operating system internals

e. Wide Scale System Analysis

Description: Wide scale system analysis is the competency of looking at rudimentary host system telemetry from a breadth of systems for the purpose of identifying anomalous activity. Wide scale system analysis is distinct from host system forensic analysis primarily in the number of systems being analyzed. The intent of this analysis is to identify additional systems showing indications of adversary presence using behavioral/anomaly detection techniques or leveraging indicators of compromise derived from other incident related analysis. Special attention is paid to how an adversary maintains persistence, leverages access credentials, and how this is leveraged to access other systems or resources on the network.

Critical Tasks:

- Frequency Analysis
- Whitelisting/Blacklisting
- Anomaly Detection
- Memory Triage

Annex J: Acronym List

CSA – Cybersecurity Advisor
CS&C – (Department of Homeland Security) Office of Cybersecurity and Communications
CI – Critical Infrastructure
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
DoD – Department of Defense
DoDIN – Department of Defense Information Network
DOJ – Department of Justice
DOS – Department of State
DSCA – Defense Support of Civil Authorities
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
IC SCC – Intelligence Community Security Coordination Center
ICE – (Department of Homeland Security) Immigrations and Customs Enforcement
ICT – Information and Communications Technology
IP – (Department of Homeland Security) Office of Infrastructure Protection
ISAC – Information Sharing and Analysis Center
ISAO – Information Sharing and Analysis Organization
JOC – Joint Operations Center
LEGATs – (Federal Bureau of Investigations) Legal Attaché offices
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
NCISS – National Cyber Incident Severity Schema
NCIJTF – (Federal Bureau of Investigations) National Cyber Investigative Joint Task Force
NCPA – National Cybersecurity Protection Act
NCTOC – National Security Agency Central Security Service Cybersecurity Threat Operations Center
NICC – (Department of Homeland Security) National Infrastructure Coordinating Center
NIMS – National Incident Management System
NIST – National Institute of Standards and Technology
NIPP – National Infrastructure Protection Plan
NPS – National Preparedness System
NRF – National Response Framework
NSA/CSS – National Security Agency/Central Security Service
NSC – National Security Council
ODNI – Office of the Director of National Intelligence
PII – Personally Identifiable Information

PSA – Protective Security Advisor
PPD – Presidential Policy Directive
SCC – Sector Coordinating Council
SLTT – State, Local, Tribal, and Territorial
SLTTGCC – State, Local, Tribal, and Territorial Government Coordinating Council
SSA – Sector Specific Agency
UCG – Unified Coordination Group
USCYBERCOM – (Department of Defense) United States Cyber Command
USSS – (Department of Homeland Security) United States Secret Service