Annex A: Authorities and Statutes

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

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

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

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

Annex B: Cyber Incident Severity Schema

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

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

Figure 1 below depicts several key elements of the schema.

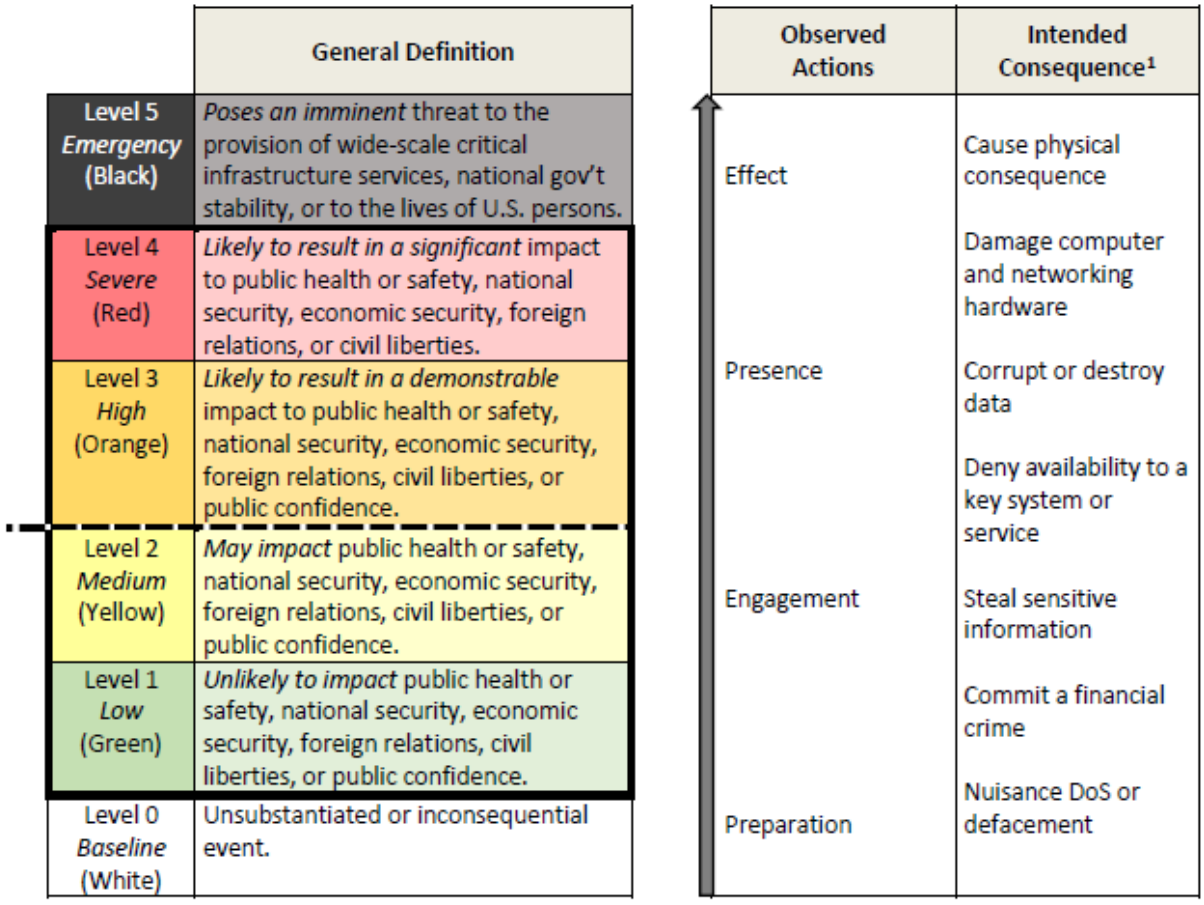

Figure 1: Elements of the Cyber Incident Severity Schema

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 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 1: Key Federal Points of Contact

<table>
<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)
(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: cywatch@ic.fbi.gov or (855) 292-3937
▪ Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.</td></tr>
</table>

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

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

Annex E: Roles of Federal Cybersecurity Centers

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

National Cybersecurity and Communications Integration Center (NCCIC)

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

National Cyber Investigative Joint Task Force (NCIJTF)

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

Cyber Threat Intelligence Integration Center (CTIIC)

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

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

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

National Security Agency Cybersecurity Threat Operations Center (NCTOC)

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

Department of Defense Cyber Crime Center (DC3)

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

[41] See page 30 for description.

Intelligence Community – Security Coordination Center (IC-SCC)

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

Annex F: Core Capabilities and Critical Tasks

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

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

Core Capabilities and Critical Tasks
3. Forensics and Attribution **Description:** Forensic investigations and efforts to provide attribution for an incident are complementary functions that often occur in parallel during a significant cyber incident.
Critical Tasks: • Retrieve digital media and data network security and activity logs. • Conduct digital evidence analysis, and respecting chain of custody rules. • Conduct physical evidence collections, analysis adhere to rules of evidence collection as necessary. • Assess capabilities of likely threat actors(s). • Leverage the work of incident responders and technical attribution assets to identify malicious cyber actor(s). • Interview witnesses, potential associates, and/or perpetrators if possible. • Apply confidence levels to attribution assignments. • Include suitable inclusion and limitation information for sharing products in attribution elements guidance. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Perform audit activities to verify and validate security mechanisms are performed as intended.
4. Infrastructure Systems **Description:** Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity.
Critical Tasks: • Maintain a comprehensive understanding of the needs for the safe operation of control systems. • Stabilize and regain control of infrastructure. • Increase network isolation to reduce the risk of a malicious cyber activity propagating more widely across the enterprise or among interconnected entities. • Stabilize infrastructure within those entities that may be affected by cascading effects of the cyber incident. • Facilitate the restoration and sustainment of essential services (public and private) to maintain community functionality. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Maintain up-to-date data knowledge of applicable emerging and existing security research, development, and solutions.

Core Capabilities and Critical Tasks
5. <u>Intelligence and Information Sharing</u> **Description:** Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as necessary.
Critical Tasks: • Monitor, analyze, and assess the positive and negative impacts of changes in the operating environment as it pertains to cyber vulnerabilities and threats. • Share analysis results through participation in the routine exchange of security information—including threat assessments, alerts, threat indications and warnings, and advisories—among partners. • Confirm intelligence and information sharing requirements for cybersecurity stakeholders. • Develop or identify and provide access to mechanisms and procedures for confidential intelligence and information sharing between the private sector and government cybersecurity partners.[42] • Use intelligence processes to produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include critical infrastructure participants and partners with roles in physical response efforts. • Share actionable cyber threat information with SLTT and international governments and private sectors to promote shared situational awareness. • Enable collaboration via online networks that are accessible to all participants. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

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

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

Core Capabilities and Critical Tasks
8. Operational Communications **Description:** Ensure the capacity for timely communications in support of security, situational awareness, and operations, by any and all means available, among and between entities affected by the malicious cyber activity and all responders.
Critical Tasks: • Ensure the capacity to communicate with both the cyber incident response community and the affected entity. • Establish interoperable and redundant voice, data, and broader communications pathways between SLTT, particularly state fusion centers, federal, and private sector cyber incident responders. • Facilitate establishment of quickly formed ad hoc voice and data networks on a local and regional basis so critical infrastructure entities can coordinate activities even if Internet services fail. • Coordinate with any UCG (or entity) established to manage physical (or non-cyber) effects of an incident. Ensure availability of appropriate secure distributed and scalable incident response communication capabilities including out-of-band communications mechanisms where traditional communications and/or systems are compromised. Adhere to appropriate mechanisms for safeguarding sensitive and classified information private sector personnel should obtain the necessary clearances and accesses to facilitate the quick sharing of information. • Protect individual privacy, civil rights, and civil liberties. • Cyber threat information also is conducted through automated indicator sharing using established formats such as Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information (STIX/TAXII).[43] • Perform red team activities to verify and validate that forensics and attribution capabilities are performing as intended and have adequate visibility.
9. Operational Coordination **Description:** Establish and maintain a unified and coordinated operational structure and process that appropriately integrate all critical stakeholders and support execution of core capabilities.
Critical Tasks: • Mobilize all critical resources and establish coordination structures as needed throughout the duration of an incident. • Define and communicate clear roles and responsibilities relative to courses of action. • Prioritize and synchronize actions to ensure unity of effort. • Ensure clear lines and modes of communication between entities, both horizontally and vertically. • Ensure appropriate private sector participation in operational coordination throughout the cyber incident response cycle consistent with the NIPP. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Perform table-top activities to verify and validate effective and appropriate coordination between stakeholders.

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

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

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

Core Capabilities and Critical Tasks
11. <u>Public Information and Warning</u> **Description:** Deliver coordinated, prompt, reliable, and actionable information to the whole community and the public, as appropriate, through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threat or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.
Critical Tasks: • Establish accessible mechanisms and provide the full spectrum of support necessary for appropriate and ongoing information sharing among all levels of government, the private sector, faith-based organizations, nongovernmental organizations, and the public. • Share actionable information and provide situational awareness with the public, private, and nonprofit sectors, and among all levels of government. • Leverage all appropriate communication means, such as the Integrated Public Alert and Warning System, public media, and social media sites. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect applicable information sharing and privacy protections, including Traffic Light Protocol. • Assure availability of redundant options to achieve critical public information, threat indication, and warning outcomes.
12. <u>Screening, Search, and Detection</u> **Description:** Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence.
Critical Tasks: • Locate persons and networks associated with cyber threats. • Develop relationships and further engage with critical infrastructure participants (private industry and SLTT partners). • Conduct physical and electronic searches as authorized by law • Collect and analyze information provided. • Detect and analyze malicious cyber activity and support mitigation activities. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.

Core Capabilities and Critical Tasks
13. Situational Assessment **Description:** Provide all decision makers with decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response.
Critical Tasks: • Coordinate the production and dissemination of modeling and effects analysis to inform immediate cyber incident response actions. • Maintain standard reporting templates, information management systems, essential elements of information, and critical information requirements. • Develop a common operational picture for relevant incident information shared by more than one organization. • Coordinate the structured collection and intake of information from multiple sources for inclusion into the assessment processes. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
14. Threats and Hazards Identification **Description:** Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of an entity.
Critical Tasks: • Identify data requirements across stakeholders. • Develop and/or gather required data in a timely and efficient manner to accurately identify cyber threats. • Ensure that the right people receive the right data at the right time. • Translate data into meaningful and actionable information through appropriate analysis and collection tools to aid in preparing the public. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Discover, evaluate and resolve gaps in policy, facilitate or enable technologies, partnerships, and procedures which are barriers to effective threat, vulnerability, and hazard identification for the sectors.

Annex G: Developing an Internal Cyber Incident Response Plan

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

National Operational Planning

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

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

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

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

Response Operational Planning

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

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

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

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

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

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

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

Application

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

Developing an Internal Cyber Incident Response Plan

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Annex I: Additional Resources

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

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

Annex J: Acronym List

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

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