# National Cyber Incident Response Plan Update
# Public Comment Draft

**About this draft:** This is a pre-decisional draft for public comment. It does not represent the final position of the U.S. Government or any participant in the process and is continuing to undergo updates as feedback is received.

**Publication: December 2024**

**Information Cutoff: Links, contact information, and references in this document are current as of October 2024.**

**Cybersecurity and Infrastructure Security Agency**

## Contents

# Executive Summary

The 2023 National Cybersecurity Strategy called for an update of the 2016 National Cyber Incident Response Plan (NCIRP), a strategic national framework for how federal; private sector; state, local, tribal, and territorial (SLTT); and international partners collectively address cyber incidents under Presidential Policy Directive 41 (PPD-41). This update responds to changes in the cyber threat landscape, federal law and policy, and new organizational capabilities.

At a high level, the NCIRP sets out the structures that the United States government will use to coordinate the response to cyber incidents. It also provides a framework for the potential roles of federal agencies, SLTT government, the private sector, and civil society. However, the NCIRP is not a step-by-step instruction manual on how to conduct a response effort—nor could it be, as every incident and every response is different. Rather, the NCIRP sets out a flexible structure that responders can use to shape their efforts and maximize both efficiency and coordination. CISA encourages private sector entities to review the NCIRP to understand how the government will partner with them in an incident and how to incorporate this framework into their own planning efforts.

The NCIRP describes four lines of effort: Asset Response, Threat Response, Intelligence Support, and Affected Entity Response. The NCIRP also includes coordination mechanisms, key decision points, and priority activities across the cyber incident response lifecycle.

The NCIRP identifies coordinating structures that response stakeholders may leverage for cyber incidents requiring cross-sector, public-private, or federal coordination. Two key coordination structures are defined by PPD-41: the Cyber Response Group (CRG) for incident response policy and awareness and the Cyber Unified Coordination Group (Cyber UCG) for incident response coordination. The lead agencies for each federal line of effort manage coordination and resourcing within each line of effort.

The NCIRP distinguishes between two main cyber incident response phases: Detection and Response. The Detection phase encompasses monitoring, analysis, and detection to validate a reported incident and assess whether it rises to the level of a significant cyber incident. The Response phase encompasses activities to contain, eradicate, and recover from incidents, and to carry out law enforcement and intelligence activities necessary to attribute the incident and hold the perpetrators accountable.

Comprehensive national preparedness for cyber incidents requires additional planning to address more specific issues and stakeholder communities than the NCIRP alone can provide. The Cybersecurity and Infrastructure Security Agency (CISA) will develop and support additional planning documents to meet these needs. CISA plans to implement a regular cycle of revisions to fulfill its statutory responsibility to update, maintain, and exercise the NCIRP.

# Introduction

The NCIRP is a strategic national framework for how federal, private sector, SLTT, and international partners address cyber incidents as defined in Presidential Policy Directive 41—U.S. Cyber Incident Coordination (PPD-41) when the incident, or a group of related incidents, has a severity at or above Level 2 of the Cyber Incident Severity Schema.[1] This Plan supports continuous improvement of national cyber incident response capabilities by leveraging CISA's statutory responsibility to update the NCIRP.[2]

---

*"…Chinese cyber actors, including a group known as "Volt Typhoon," are burrowing deep into our critical infrastructure to be ready to launch destructive cyber-attacks in the event of a major crisis or conflict with the United States."*

*CISA Director Jen Easterly*
*Before the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party*
*January 31, 2024*

---

At a high level, the NCIRP describes the lines of effort and stakeholders, coordinating mechanisms, and key decisions and activities across the cyber incident response lifecycle that the U.S. government will use to coordinate response to cyber incidents. These types of incidents are defined in **Table 1**. The NCIRP is intended to promote national unity of effort by providing a framework that harnesses the contributions of many stakeholders in detecting and responding to cyber incidents. It is not a step-by-step procedure for conducting a cyber incident response, as every incident and response is different. This document provides a flexible framework that responders can use to coordinate their efforts to maximize effectiveness. While voluntary for all stakeholders outside the federal government, CISA encourages private sector, SLTT government, and all other non-federal stakeholders to review the NCIRP to understand how the U.S. government will partner with them in cyber incident response, and to incorporate this framework into their own planning efforts, including preparatory activities outlined in **Annex B**.

The NCIRP is designed for coordinating detection and response to cyber incidents. However, cyber incidents may cause consequences outside the cyber domain, like disrupting critical infrastructure operations, damaging equipment, or threatening public health and safety. The NCIRP is applicable only to the cyber component of such incidents and supports other processes designed to manage consequences outside the cyber domain, such as those established under Homeland Security

[1] The Cyber Incident Severity Schema (described in **Annex A**) is a national framework for evaluating the severity of cyber incidents. At severity Level 2 of the schema, response may involve some of the coordinating structures and response lines of effort described in this document based on the scope and scale of the response required. When an incident is at severity Level 3 or above it is a significant cyber incident and will typically require the full implementation of the NCIRP Update's coordinating structures and response lines of effort.

[2] Cybersecurity plans. 6 USC §660(c) and (d)

Presidential Directive 5 (HSPD-5)--Management of Domestic Incidents or other federal or non-federal authorities. To integrate cyber and physical incident response per PPD-41, the NCIRP leverages doctrine from the Federal Emergency Management Agency's National Response Framework, the National Incident Management System, and the Incident Command System.

*Table 1: Cyber Incident Definitions from PPD-41*

| Incident | Definition |
|---|---|
| Cyber Incident | An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. A cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. |
| 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.[3] |

## Lines of Effort

PPD-41 organizes national cyber incident response into four lines of effort (LOE) that capture the fundamental sets of roles and responsibilities involved in a holistic response, recognizing that no one stakeholder or federal agency can meet all the needs involved. These LOEs are Asset Response, Threat Response, Intelligence Support, and Affected Entity Response (see **Figure 1**).

[3] Note that incidents affecting federal networks that meet the threshold for a "major incident" under the Federal Information Security Modernization Act of 2014 or in Office of Management and Budget guidance are also significant cyber incidents under PPD-41 (PPD-41 Annex, Section III)

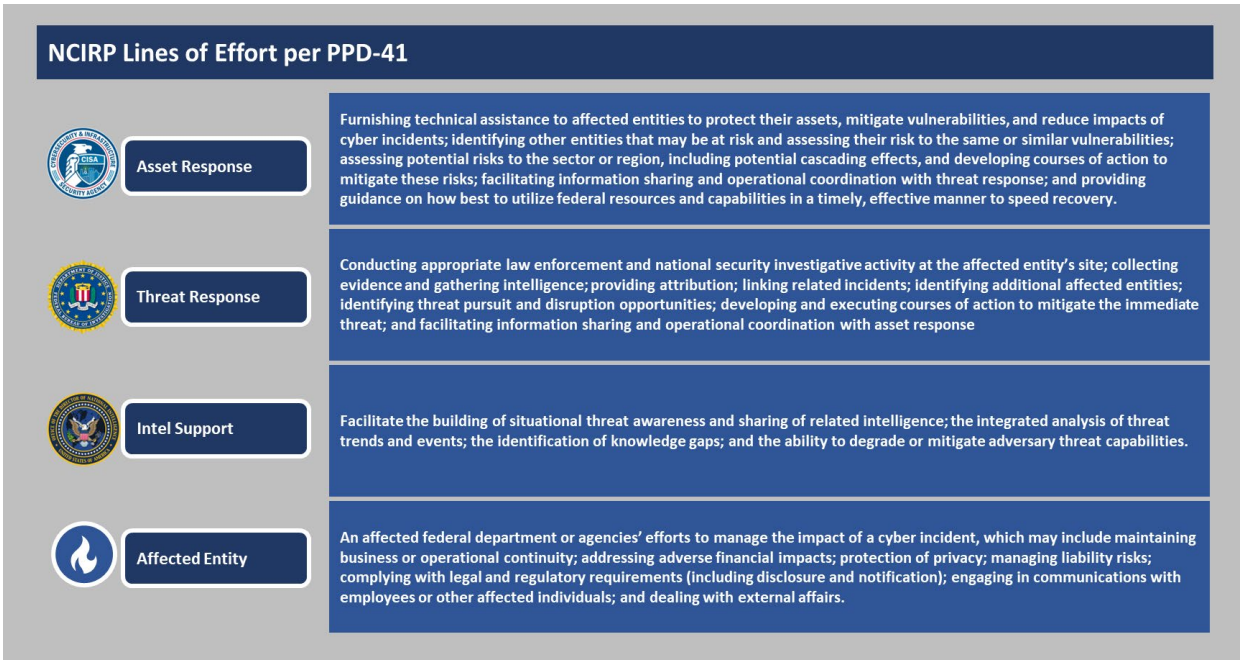


*Figure 1. Federal Lines of Effort and Lead Agencies*

The leads for each LOE are:

- **Asset Response:** CISA leads coordinated efforts for assisting affected entities with protection of their assets.[4]
- **Threat Response:**
  - The Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI), FBI-designated field offices, and National Cyber Investigative Joint Task Force (NCIJTF) are the primary law enforcement entities that develop and implement threat response.
  - U.S. Secret Service and other law enforcement entities also investigate cybercrime and contribute to threat response as needed within their jurisdictions.[5]
- **Intelligence Support:** The Office of the Director of National Intelligence (ODNI), through the Cyber Threat Intelligence Integration Center (CTIIC), leads coordinated intelligence support in response to a cyber incident.
- **Affected Entity:**
  - When a cyber incident affects federal departments or agencies, each affected department or agency is responsible for leading and resourcing its own cyber incident response in coordination with CISA—or in the case of Department of Defense (DOD) or Intelligence Community (IC) entities, U.S. Cyber Command (USCYBERCOM) or the IC Security Coordination Center (IC SCC), respectively.

[4] US Cyber Command leads Asset Response for incidents affecting the Department of Defense Information Network and the Intelligence Community (IC) Security Coordination Center leads Asset Response for incidents affecting the IC Information Environment.

[5] US Cyber Command leads Threat Response for incidents affecting the Department of Defense Information Network and the Intelligence Community (IC) Security Coordination Center leads Threat Response for incidents affecting the IC Information Environment.

- When a cyber incident affects a private entity, the federal government typically does not play a role in this line of effort but does remain cognizant of the affected entity's response activities, consistent with the principles established in PPD-41.

A variety of additional stakeholders participate in one or more LOEs, bringing their capabilities to bear in coordination with federal leads to manage cyber incidents. These include the DOD, other law enforcement agencies, Sector Risk Management Agencies (SRMAs), other SLTT government agencies, Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs), and affected entities. The roles of lead agencies and other stakeholders in each LOE are described further in Annex D.

## Coordinating Structures

Unified cyber incident response requires coordinating structures to harness the relevant capabilities and authorities of all public and private stakeholders across all incident phases. This section describes the coordination mechanisms and structures that currently exist, or are authorized, and play an on-going and continuous role in cyber incident response. The following section will describe when and how these structures are integrated across each phase of cyber incident response.

Table 2 provides a summary of the existing coordinating structures that may be involved in cyber incident response, the coordinating lead organization, and the purpose of each.

***Table 2: Coordinating Structures Involved in Cyber Incident Response***

| Name | Coordinating Lead Organization | Purpose in Cyber Incident Response |
|---|---|---|
| Cyber Response Group (CRG) | Executive Office of the President | Coordinates 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. Its functions during a cyber incident include:<br>▪ Receiving updates from federal agencies and measures being taken to resolve or respond<br>▪ Resolving issues elevated to it by subordinate bodies such as the Cyber UCG<br>▪ Collaborating with other groups in the National Security Council (NSC) when a cross-disciplinary response is required |

| Name | Coordinating Lead Organization | Purpose in Cyber Incident Response |
|---|---|---|
| | | ▪ Identifying and considering options for response and making recommendations to the Deputies Committee when higher level guidance is required<br>▪ Considering the policy implications for public messaging<br>▪ Coordinating a communications strategy as necessary |
| Cyber Unified Coordination Group (Cyber UCG) | Participation will regularly include:<br>▪ CISA, FBI, CTIIC as LOE leads<br>▪ SRMAs for affected critical infrastructure sectors<br>▪ Affected federal departments or agencies<br>▪ Other responding federal agencies<br>May include non-federal participation in limited circumstances.<br>CISA may serve as an executive secretariat for the Cyber UCG to support its operations. | Per PPD-41, the Cyber UCG serves as the primary national operational coordination mechanism between and among federal agencies, responsible for identifying and developing response plans and activities during significant cyber incidents. The Cyber UCG is a task organization of federal entities that primarily identifies and coordinates response activities across the asset response, threat response, intelligence support, and affected entity response LOEs. Functions include identifying operational objectives, determining resource needs, and coordination of activities needed to achieve cyber incident response objectives. Non-federal input or participation is tailored based on the incident. |

| Name | Coordinating Lead Organization | Purpose in Cyber Incident Response |
|---|---|---|
| Sector Risk Management Agencies (SRMAs) | Each SRMA (or co-SRMAs in coordination with each other) for their sector | Manages sector risks before and during an incident. Provides sector-specific expertise to the Cyber UCG and other stakeholders. Provides assistance to affected industry entities as appropriate. Coordinates with CISA, as the National Coordinator for critical infrastructure and resilience and the lead agency for asset response, the IC, and other relevant federal departments and agencies on incident response; Government Coordinating Councils, Sector Coordinating Councils, ISACs and ISAOs, critical infrastructure owners and operators; and, where appropriate, independent regulatory agencies and SLTT entities.[6] |

[6] During a cyber incident, SRMAs may have additional responsibilities for consequence management stemming from the cyber incident, but that are carried out through processes outside the scope of the NCIRP.

| Name | Coordinating Lead Organization | Purpose in Cyber Incident Response |
|---|---|---|
| Joint Cyber Defense Collaborative (JCDC) | CISA | As a public-private partnership, the JCDC brings together federal and non-federal partners to address cyber incidents through collaborative planning, information sharing, development of mitigation guidance, and other operational activities relevant to asset response. CISA leverages the JCDC and its collaborative processes to allow all relevant asset response stakeholders (including participants that are not JCDC members) to work together to resolve specific incidents as required. |
| ISACs/ISAOs | Individual ISACs/ISAOs | Collect, analyze, and disseminate actionable threat information to members and provides them with tools to mitigate risks and improve resilience.<br>ISACs and ISAOs are private sector entities that facilitate the sharing of cyber threat information and best practices among their members and work with the Department of Homeland Security (DHS) and related SRMAs to support incident response activities. |

## Phases of Cyber Incident Response Operations

This section describes how public and private sector stakeholders work together to detect and respond to cyber incidents, using the roles and coordinating structures mentioned above. This plan (1) better enables the implementation of a unified national response and (2) more effectively coordinates the processes to assess the severity of incidents, including determination that a significant incident is occurring or imminent. While the phases are generally sequential, some activities will overlap.

The Cyber Incident Severity Schema, described in **Annex A**, guides the federal evaluation of the severity and significance of an incident. The schema is leveraged by the CRG, federal departments and agencies, and other federal coordination structures to help determine the severity of the incident. Non-federal stakeholders are encouraged to be familiar with and make use of the schema, as well. The activities and decision points outlined in the following sections begin to apply when an incident reaches severity level two. Incidents designated as level three or above are considered Significant Cyber Incidents in accordance with PPD-41 and may trigger additional activities, such as the establishment of a Cyber UCG.

The decisions and activities described below reflect activities and coordination structures that occur across the LOEs. Since every cyber incident has unique characteristics, the detection and response phases below may be adapted to best handle each incident.

## Detection Phase

**Purpose:** Detection encompasses a broad set of continuous monitoring and analysis activities. Active engagement with service providers, the cybersecurity community, and critical infrastructure owners and operators is critical to detect and validate the severity of an incident. While detection-related activities are always ongoing, for NCIRP purposes this phase begins when a cyber incident is identified which could warrant implementing the NCIRP.

**Key Decisions and Activities: Table 3** outlines key decisions that could be made during the detection phase of a cyber incident, as well as the coordinating structure(s) associated with the decision. **Table 4** outlines key coordinated activities in this phase by LOE.

***Table 3. Key Decisions - Detection Phase***

| Key Decision | Why It Matters | Information Supporting Decision | Decision Mechanism |
|---|---|---|---|
| Determine severity of the cyber incident | ▪ Informs level of effort and resource commitments needed<br>▪ May inform significant incident declaration process under the Cyber Response and Recovery Act | ▪ Impact to the nation<br>▪ Threat intelligence<br>▪ Geopolitical context<br>▪ SRMA domain expertise | Consensus of CRG agencies.<br>NSC when CRG agencies disagree |

| Key Decision | Why It Matters | Information Supporting Decision | Decision Mechanism |
|---|---|---|---|
| Determine if CISA should convene an incident-specific group of stakeholders through the JCDC to coordinate asset response activities across stakeholders | ▪ Creates a scalable and predictable structure for the detection, and if needed, response processes<br>▪ Promotes unity of effort across public and private sectors | ▪ Input from stakeholders collaborating on detection and analysis<br>▪ Number and criticality of stakeholders involved | CISA in collaboration with other detection and response stakeholders |
| Determine if a Cyber UCG, or other coordinating mechanism, is needed | ▪ Identifies a need for greater coordination between agencies exercising their existing authorities in response to an incident<br>▪ Requires executive-level engagement from responding federal agencies, including SRMAs<br>▪ Promotes governmental unity of effort with respect to incident response | ▪ Severity of incident<br>▪ Scale of incident<br>▪ Complexity of coordination needed<br>▪ Number of agencies involved | NSC, CRG, consensus of two or more CRG agencies, or when the Secretary of Homeland Security makes a determination based on PPD-41(V)(B)(b)[7] |

[7] PPD-41(V)(B)(b) provides that "A Cyber UCG shall also be formed 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."

*Table 4. Coordinated Activities - Detection Phase*

| Coordinated Activity | Core Participants | Why Coordinate | Intended Outcome of Activity |
|---|---|---|---|
| Engage key private sector stakeholders to contribute to further understanding incident | ▪ CISA, leveraging the JCDC<br>▪ SRMAs | ▪ Leverage private sector information and expertise in assessing scale and scope of incident | ▪ Increased comprehensive situational awareness about the incident |
| Identify and acquire priority information needs | ▪ CISA<br>▪ DOJ/FBI<br>▪ ODNI<br>▪ SRMAs<br>▪ Other stakeholders participating in response | ▪ Focus information gathering, information sharing, and intelligence efforts | ▪ Develop the information needed for collaborative analysis to understand the scale, scope, and impact of the cyber incident |
| Conduct collaborative risk and impact assessment and share results | ▪ CISA<br>▪ SRMAs<br>▪ DOJ/FBI<br>▪ ODNI | ▪ Leverage and share the insights and analytical capabilities available across the stakeholder community | ▪ Form a unified and comprehensive as possible picture of the nature, scale, scope, and impact of the incident<br>▪ Support attribution |

| | | | |
|---|---|---|---|
| Understand scope and impact of incident | ▪ CISA<br>▪ DOJ/FBI<br>▪ ODNI<br>▪ SRMAs<br>▪ Responding ISACs/ISAOs<br>▪ Relevant Vendors<br>▪ Other stakeholders with high visibility into affected portions of ecosystem (e.g., Internet Service Providers, managed service providers, cloud providers) | ▪ For major incidents, no one stakeholder has a comprehensive view<br>▪ Insights of multiple stakeholders usually needed to form a complete and accurate picture of an incident and its impacts | ▪ Shared understanding of how "big" the incident is in terms of number of affected stakeholders, severity of impact, and effort needed to remediate and recover<br>▪ Understand cross-sector impacts and risks |

## Response Phase

**Purpose:** Response encompasses activities to contain, eradicate, and recover from incidents, and to carry out law enforcement investigations and intelligence activities. Response activities within the scope of the NCIRP are focused on the cybersecurity aspects of the incident, while broader consequence management (including impacts to people and physical infrastructure) will be handled by other processes and will generally be coordinated through a Unified Coordination Group (UCG) organized under HSPD-5.

**Key Decisions and Activities: Table 5** outlines key decisions to make during response to a cyber incident, as well as the coordinating structures associated with the decision. **Table 6** outlines key coordinated activities in this phase.

***Table 5. Key Decisions-Response Phase***

| Key Decision | Why It Matters | Information Supporting Decision | Decision Mechanism |
|---|---|---|---|
| Determine key non-governmental stakeholders to contribute to solution development and implementation | ▪ Identifies the technical expertise and services that are available in the private sector | ▪ Relevant technical expertise and reach<br>▪ Likelihood of effectiveness | ▪ CISA in coordination with the CRG/Cyber UCG, other LOE leads and SRMAs |

| | | | |
|---|---|---|---|
| Determine shared priorities for response | ▪ Promotes unity of effort across stakeholders<br>▪ Ensures most important activities are the focus | ▪ Scope and impact of incident<br>▪ Response options and resources available<br>▪ National leadership priorities<br>▪ Overall context of the situation | ▪ Cyber UCG |
| Determine when and how to implement response activities | ▪ Promotes unity of effort and deconfliction coordination<br>▪ Synchronizes response activities for maximum effectiveness | ▪ Capabilities stakeholders have and when they can be implemented<br>▪ Understanding of incident dynamics | ▪ LOE leads in coordination with one another, and when activated, the Cyber UCG |
| Determine whether otherwise available resources, other than the Cyber Response and Recovery Fund (CRRF), are likely insufficient to effectively respond or mitigate the incident | ▪ Resource insufficiency is one of the requirements for a significant incident declaration and access to the CRRF<br>▪ The CRRF can provide additional resources to support incident response if otherwise available resources are insufficient | ▪ Assessment of the requirements for incident response and comparison with available resources | ▪ CISA coordinates requests for Secretary of DHS determination in consultation with the National Cyber Director |
| Determine conditions for ending the incident response phase | ▪ Indicates federal response coordination is no longer needed | ▪ Effectiveness of response activities<br>▪ Full scope of incident<br>▪ Status of incident response stakeholder capabilities and operational state | ▪ LOE leads in coordination with one another, or when activated, the Cyber UCG |

*Table 6. Coordinated Activities-Response Phase*

| Coordinated Activity | Core Participants | Why Coordinate | Intended Outcome of Activity |
|---|---|---|---|
| Identify information and support needs of the affected entities and other key stakeholders | ▪ CISA<br>▪ DOJ/FBI<br>▪ ODNI<br>▪ SRMAs | ▪ Establish lines of communication<br>▪ Enable information sharing, containment, and further detection and response actions<br>▪ Prioritize LOE activities | ▪ Affected entities and other key stakeholders are able to communicate and collaborate with appropriate federal agencies<br>▪ Federal engagement with affected entities occurs in a coordinated way |
| Develop initial coordinated response options and priorities | ▪ CISA coordinates the development of response options for asset response in coordination with SRMAs, other LOE leads, affected entities, and other stakeholders convened for the incident through the JCDC | ▪ Better understand the extent of the incident and support immediate containment activities | ▪ Reduced risk of greater impact<br>▪ Set conditions for further remediation |
| Develop strategy for implementing, synchronizing, and measuring the effectiveness of response activities | ▪ CISA<br>▪ DOJ/FBI<br>▪ ODNI<br>▪ SRMAs<br>▪ Other relevant stakeholders as determined by LOE leads | ▪ Transition from immediate containment to more comprehensive response<br>▪ Identify initial measures of effectiveness for different response activities | ▪ Nationally coordinated incident response effort<br>▪ Facilitates transition from detection phase to response phase |

| | | | |
|---|---|---|---|
| Develop mitigation guidance | ▪ CISA, DOJ/FBI, ODNI, SRMAs, and other federal agencies with relevant expertise<br>▪ Responding ISACs/ISAOs<br>▪ Relevant product vendors<br>▪ Incident response firms/teams<br>▪ Other technically capable affected or at-risk entities | ▪ There are often multiple ways to mitigate an incident, and different stakeholders may identify differing approaches<br>▪ Initial mitigation guidance is often improved upon by others | ▪ Mitigation guidance is developed, validated, and published |
| Publish and amplify mitigation guidance | ▪ CISA, DOJ/FBI, ODNI, SRMAs, and other federal agencies with relevant expertise<br>▪ Responding ISACs/ISAOs<br>▪ Relevant product vendors<br>▪ Private sector incident response firms/teams | ▪ Ensure accurate and consistent guidance is available across multiple communications channels<br>▪ Maximize speed and reach of publication by leveraging the communications channels and audiences available to different stakeholders | ▪ Mitigation guidance is widely available from trustworthy sources |
| Information sharing and operational coordination with international government partners | ▪ CISA<br>▪ Department of State<br>▪ DOJ/FBI<br>▪ ODNI<br>▪ SRMAs | ▪ Ensure coordinated messaging across U.S. government agencies<br>▪ Leverage all relevant partnerships available across the U.S. government | ▪ All relevant partners are effectively engaged for an incident |

| | | | |
|---|---|---|---|
| | | ▪ Ensure unity of effort with international partners | |
| Investigate and identify perpetrating threat actors | ▪ DOJ/FBI<br>▪ Other law enforcement<br>▪ CISA<br>▪ ODNI<br>▪ SRMAs | ▪ Information gained through asset response or intelligence activities may contribute to threat response<br>▪ Information gained in investigation may be relevant to other lines of effort | ▪ Law enforcement can identify and further pursue and/or prosecute perpetrating threat actors |
| Disrupt threat actors | ▪ DOJ/FBI<br>▪ Other law enforcement<br>▪ DOD<br>▪ ODNI<br>▪ CISA<br>▪ Technology ecosystem companies or other non-governmental entities, as appropriate | ▪ Various U.S. government agencies have capabilities relevant to disrupting threat actor activity<br>▪ At times, technology ecosystem companies or other non-governmental stakeholders may have relevant capabilities to disrupt threat actors | ▪ Threat actor capabilities are degraded or destroyed |

**Cross-cutting Activities:** LOE lead agencies, SLTT, and private sector stakeholders will undertake some common actions, although most response activities are likely to occur within the authorities and capabilities of the LOE lead agencies after the Cyber UCG coordination. Some common actions could be:

- Contributing to prioritization and adjudication of response options across the LOEs
- Working to restore critical services as quickly as possible

- Determining the effectiveness of response activities and identifying criteria for ending significant response activities

**Coordination Considerations:**

**CRG:** The CRG coordinates the development and implementation of U. S. government policy and strategy, including providing White House-level direction on priorities and resolution of disputes that are not resolved within the Cyber UCG.

**Cyber UCG:** The Cyber UCG is the primary national operational coordination mechanism for federal agencies responsible for identifying, developing, and coordinating response plans and activities during a significant cyber incident. The Cyber UCG coordinates operational activities in alignment with U. S. government policy and strategy developed and implemented by the CRG.

**Regional Coordination:** At the regional level, SLTT and private sector coordination structures for containment and eradication also integrate with federal coordinating structures. Because SLTT entities use different approaches to manage cyber incidents, there is no one-size-fits-all solution for federal-SLTT coordination.

**Messaging:** Unified and reliable messaging is also integral to successful response during a cyber incident. When public messaging is necessary, participants of the Cyber UCG, other government partners, and relevant private sector entities, such as affected entities, should seek to align messaging as appropriate.

**Enhanced Coordination Procedures:** Enhanced coordination procedures are a mechanism required by PPD-41 to enhance federal agencies' abilities to respond to significant cyber incidents. PPD-41 requires federal agencies that regularly participate in the CRG, including SRMAs, to create and maintain internal enhanced coordination procedures. These procedures are designed to enable federal agencies to plan for and implement the capability to increase their operational pace for coordination in determining and responding to a significant national cyber incident. Per PPD-41, enhanced coordination procedures should facilitate the activation, prioritization, and management of federal resources and priorities during a significant cyber incident to enable federal agencies to implement their national cyber incident response responsibilities, including engaging private sector and SLTT stakeholders.

Enhanced coordination procedures for significant cyber incidents will generally be activated when agencies determine that a cyber incident exceeds their normal cyber operating capacities and authorities, or when a Cyber UCG is formed. These procedures require the assignment of dedicated leadership, supporting personnel, available facilities (physical and communications), and internal processes that will enable it to increase its coordination within and outside of its designated sector.

Enhanced coordination procedures help to:

- Facilitate communication and coordination pathways between other federal agencies and stakeholders during a significant cyber incident, including the relevant agency points-of-contact, and notify the CRG that enhanced coordination procedures were activated or initiated.
- Support internal and external communications and decision making processes that are consistent with effective incident coordination.

- Initiate the development of standard procedures, exercises, and other processes for maintaining these procedures.

## Post-Incident Activities

Following a cyber incident, multiple activities may follow depending on the circumstances of the incident.

After a significant cyber incident for which a Cyber UCG was formed, the Chair of the CRG shall direct a review of the Cyber UCG's response and prepare a report within 30 days. Federal agencies are to modify any plans or procedures for which they are responsible, as appropriate or necessary, considering that report.[8]

A declaration of a significant incident by the Secretary of Homeland Security under the Cyber Response and Recovery Act terminates 120 days after the declaration or last renewal (unless the Secretary determines earlier that the declaration is no longer needed). CISA will prepare a draft report on fund allocations to Congress in accordance with statutory reporting requirements.

Additionally, Executive Order 14028 established the Cyber Safety Review Board.[9] The board integrates collaboration between public and private sector members and provides independent, strategic, and actionable recommendations to the President, the Secretary of Homeland Security, and the Director of CISA for improving cybersecurity and incident response practices and policy upon completion of the board's review of an incident.

Capturing lessons learned is essential but putting them into practice is vital. To that end, cyber incident response stakeholders should capture and implement lessons learned to the extent practicable.

## Implementation and Maintenance

As the cyber threat and cyber defense environment continues to rapidly evolve, continual preparedness is needed to coordinate effective responses to cyber incidents. CISA will lead ongoing work across the stakeholder community to exercise coordination, conduct additional planning to address more specific issues and stakeholder communities, and update the NCIRP on a predictable cycle.

### CISA Activities

Comprehensive national preparedness for significant cyber incidents requires additional planning that addresses more specific issues and stakeholder communities than this document alone can provide. CISA will develop and support additional cyber defense documents, such as enterprise incident response plans, sector-specific annexes, contingency-specific plans, or processes and procedures for specific operational needs such as resource requests. Further details on these activities are provided in **Annex E**.

[8] PPD-41 Annex at IV(E)

[9] "Cyber Safety Review Board." CISA. February 1, 2022. https://www.cisa.gov/resources-tools/groups/cyber-safety-review-board-csrb.

CISA has statutory responsibility to update, maintain, and exercise the NCIRP.[10] The updates will keep the NCIRP current with changes in the cyber threat and cyber defense environment, changes in law and policy, and lessons learned from past incidents.

### Federal Departments and Agencies

Federal departments and agencies should be prepared to lead and resource their cyber incident response and to fulfill their relevant roles and responsibilities. They should align their planning, procedures, and exercises to the NCIRP.

### Nationwide Activities

To ensure readiness to execute coordination, organizations should implement the actions in **Annex B: Preparing for Cyber Incidents**. **Annex F** provides a list of resources from a variety of federal and non-federal sources that may also be useful.

## Conclusion

Today's geopolitical environment requires the nation be prepared to handle significant cyber incidents that threaten our economy, national security, and public health and safety. An accessible and practical NCIRP is essential to harness the expertise, capabilities, and authorities of public and private sectors to tackle significant incidents. The NCIRP Update continues ongoing maturation of response to cyber incidents in the United States, building upon PPD-41 and the important roles of stakeholders from the private sector, SLTT entities, and federal agencies including SRMAs. The NCIRP enables clearer stakeholder understanding of how key actions and coordinating structures work in concert across the span of response phases.

The NCIRP is designed as a flexible incident response framework, recognizing both the continuous nature of stakeholder organizational missions and making the NCIRP more practical to help organizations smoothly transition into significant incident response if needed. Decision makers—including the federal government, SLTT governments, and the private sector—must work to harmonize their organizations incident coordination planning to engage with these structures and understand what contributions they can make to support national incident response.

To ensure useability in an evolving cyber threat environment, the actions and coordinating structures and functions laid out in this plan will be regularly tested and improved, both through exercises and lessons taken from live responses.

[10] Cybersecurity plans. 6 USC §660(c) and (d).

# Annex A: Cyber Incident Severity Schema

The Cyber Incident Severity Schema establishes a common framework for evaluating and assessing cyber incidents to ensure that all Federal departments and agencies have a common view of the severity of a given incident, the consequent urgency of response efforts, and the need for escalation to senior levels. The schema is not intended to be a quantitative cyber risk analysis tool but provides a qualitative baseline that informs discussions of the relative severity of an incident. As noted in PPD-41, no two incidents are the same and the incident severity assessment in one sector may not be the same in another. To this end, the schema also provides a baseline for tailored sector-specific schemas. Since 2016, many SRMAs have developed sector specific severity schemas based on this model. When evaluating the severity of a cyber incident, please consult applicable tailored schemas. The following figure below depicts several key elements of the NCIRP base schema.

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

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

***Figure 2: Cyber Incident Severity Schema***

**Notes:** In addition to characterizing the observed activity, one must consider the scope and scale of the incident when applying the general definitions to arrive at a severity level.

# Annex B: Preparing for Cyber Incidents

The following are additional resources for helping federal and non-federal stakeholders prepare for cyber incidents.

**Join the Joint Cyber Defense Collaborative (JCDC).** Critical infrastructure organizations and entities with cybersecurity expertise and visibility are welcome to participate in the JCDC, which is led by CISA. The JCDC leads public-private sector (or joint) cyber defense plans; drives operational collaboration and cybersecurity information fusion; publishes guidance; and provides a vital coordination point among public and private partners during response to cyber incidents.

**Get to know your CISA Cyber Security Advisor.** Critical infrastructure owners and operators, and SLTT officials, are encouraged to build relationships with CISA's regional staff, particularly their Cyber Security Advisor (CSA). CSAs provide cybersecurity assistance, including proactive preparedness and incident response support.

**Get to know your law enforcement agents.** Build relationships with federal, state, and local law enforcement (LE). The FBI is the primary federal law enforcement agency with jurisdiction over criminal cyber incidents and is the lead federal agency for cyber threat response activities. Private sector entities are encouraged to connect with the FBI prior to a cyber intrusion to learn who from their local field office to include in a cyber incident response plan, when to contact them, and to explore opportunities for the FBI to join tabletop exercises. Additionally, the U.S. Secret Service and other federal law enforcement entities also investigate certain cyber incidents. Additionally, consider contacting your local LE agency.

**Get to know your Sector Risk Management Agencies (SRMAs).** Critical infrastructure owners and operators are encouraged to build relationships with their sector's SRMA(s). SRMAs work with CISA to maintain situational awareness on threats, incidents, or events impacting their sector; share information; and provide domain-specific technical knowledge and capabilities.

**Join relevant information sharing partnerships.** Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) are private sector membership organizations that share cyber threat information and provide a variety of detection and response services. ISACs are critical infrastructure sector-specific and have established relationships with CISA and SRMAs. In contrast, ISAOs are not specifically tied to the critical infrastructure sectors. The ISAO Standards Organization provides a searchable directory of ISACs and ISAOs.

**Understand how and when to report cyber incidents.** Organizations can report cyber incidents to CISA and cybercrimes to the FBI or other law enforcement entities with jurisdiction. Critical infrastructure owners and operators may also report cyber incidents to SRMAs.

- How to report?
  - Report incidents to CISA via its web portal, email, or by calling 1-844-SAY-CISA.
  - Reports criminal incidents to the FBI via its web portal or by contacting an FBI field office.
  - Reports of cyber-enabled financial crimes may be reported to the Secret Service through the nearest field office.

Organizations may have obligations to report cyber incidents to the government under law, regulation, contract, or other legal processes or agreements. Note: The cyber incident reporting landscape is constantly evolving. This guide is not intended to provide a comprehensive overview of all possible reporting channels. Instead, this plan is intended to supplement an organization's existing cyber incident response resources with potential illustrative examples of key reporting avenues to consider. Organizations should consult with their legal counsel to identify relevant statutory, contractual, regulatory, and other legal reporting requirements that may apply at the time of the cyber incident.[11] **Annex C** contains additional information on cyber incident reporting.

**Incorporate the NCIRP into operations.** Organizations can align cyber incident response planning, procedures, and exercises to the collaborative mechanisms and cyber incident response process described in the NCIRP. Organizations can also use existing frameworks and templates, such as the National Institute of Standards and Technology (NIST) Special Publication 800-61 Rev. 2,[12] to develop and/or mature their existing procedures and further align to the NCIRP.

**Understand any regulatory obligations and relationships that may apply.** Organizations may be subject to regulatory obligations and should consult their legal counsel to understand and implement requirements that apply to preparing for, responding to, or recovering from cyber incidents and their impacts to business operations. Organizations should consider developing relationships with their regulatory entities prior to experiencing an incident.

[11] Further information about U.S. federal cyber incident reporting requirements either in effect or proposed across the U.S. federal government as of September 2023 is included at Appendix B of the DHS Report on *Harmonization of Cyber Incident Reporting to the Federal Government*, available at https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government.

[12] NIST SP 800-61https://doi.org/10.6028/NIST.SP.800-61r2. Revision 3 of this guide is set to be published after the release of the 2024 NCIRP, so certain sections of the NCIRP may not be in alignment with the new format of Rev. 3.

# Annex C: Voluntary Reporting of Cyber Incidents to the Federal Government

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

Organizations may be subject to cyber incident reporting requirements by law, regulation, policy, contract, or other legal instruments and should consult with their legal counsel to identify requirements that may apply at the time of a cyber incident. This annex is not intended to provide a comprehensive overview of all possible reporting channels or obligations. The NCIRP neither imposes new reporting requirements, nor does it relieve or alter existing or future reporting requirements under any law, regulation, policy, contract, or other legal instrument.[13]

An organization experiencing a cyber incident has multiple voluntary channels through which it may inform the federal government of the incident to request technical assistance, to report a crime, or to engage in operational collaboration. SLTT governments and foreign governments may also provide voluntary cyber incident reporting channels for similar purposes.

### *Cybersecurity and Infrastructure Security Agency (CISA)*

CISA accepts reports of cyber incidents, malware, software or industrial control systems vulnerabilities or compromises, and vulnerabilities in U.S. government websites through CISA Central. CISA also welcomes sharing of indicators of compromise and defensive measures.

- Web: https://www.cisa.gov/report
- Email: central@cisa.dhs.gov
- Phone: (888) 282-0870

Reporting cyber incidents to CISA benefits all of us across government and industry since cyber incidents have the potential to impact the economy, public health, and our national security. It also helps inform our collective understanding of the national cyber threat landscape. CISA encourages organizations to submit a report immediately with information that is available and understood at the time, and then to return to your incident report as you have new information to provide updates.

### *Federal Bureau of Investigation (FBI)*

The FBI accepts report of cyber-enabled crime, including computer intrusions or attacks, ransomware, and other cyber-enabled crimes and frauds which should be reported at: Internet Crime Complaint Center (IC3): https://www.ic3.gov

The FBI accepts reports of potential or ongoing crime, threats to life, and national security threats which should be reported at: https://tips.fbi.gov, 1-800-CALLFBI or by contacting your local field office at: https://fbi.gov/contact-us/field-offices

[13] Further information about U.S. federal cyber incident reporting requirements either in effect or proposed across the U.S. federal government as of September 2023 is included at Appendix B of the DHS Report on *Harmonization of Cyber Incident Reporting to the Federal Government*, available at https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government.

### *US Secret Service*

Secret Service Cyber Fraud Task Forces work to prevent, detect, and mitigate complex cyber-enabled financial crimes. Reports of such financial crimes may be submitted through the nearest Secret Service Field Office: https://www.secretservice.gov/contact/field-offices

# Annex D: Stakeholder Roles and Responsibilities by Line of Effort

## Asset Response

**PPD-41 Description:** Asset response includes furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery.

Federal LOE Lead Agency: CISA[14]

**Stakeholders: Table 7** describes key stakeholders and their roles in asset response.

***Table 7: Primary Entity Roles in Asset Response***

| Entity | Role(s) In Asset Response |
|---|---|
| CISA | ▪ Lead federal asset response activities.<br>▪ Maintain cyber hunt and incident response teams for the purpose of leading Federal asset response activities and providing timely technical assistance to Federal and non-Federal entities, including across all critical infrastructure sectors, regarding actual or potential security incidents, as appropriate and upon request.<br>▪ Operational lead for Federal Civilian Executive Branch (FCEB) cybersecurity.<br>▪ Provides unity of effort, leveraging the JCDC to bring together public and private sector asset response activities.<br>▪ In its National Coordinator role, identifies and analyzes cross-sector cybersecurity risks and impacts, as well as facilitates SRMA sector risk management and cybersecurity plans and activities.[15]<br>▪ A federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings.<br>▪ Provides, upon request, technical assistance, risk management support, and incident response capabilities to federal and non-federal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents. |

[14] With support from other Federal agencies, as appropriate, US Cyber Command leads Asset Response for the Department of Defense Information Network, and the Intelligence Community (IC) Security Coordination Center leads Asset Response for the IC Information Environment.

[15] CISA also serves as the SRMA for several sectors, and therefore also has SRMA responsibilities for those sectors.

| Entity | Role(s) In Asset Response |
|---|---|
| | ▪ When the DHS Secretary, in consultation with the National Cyber Director, makes a declaration of a significant incident under the Cyber Response and Recovery Act:<br>○ CISA coordinates the asset response activities of each Federal agency in response to the specific significant incident associated with the declaration; with appropriate entities, which may include public and private entities and SLTT governments with respect to the asset response activities of those entities and governments, and Federal and SLTT law enforcement agencies with respect to those agencies' investigations and threat response activities; and Federal and SLTT emergency management and response agencies.<br>○ Can use the Cyber Response and Recovery Fund to fund certain authorized activities.[16] |
| **Department of Defense** | ▪ Supports CISA's asset response activities including, as appropriate, providing technical assistance and sharing information to support incident mitigation.<br>▪ Provides cybersecurity assistance to Defense Industrial Base (DIB) entities and service providers upon request through multiple DOD entities.<br>▪ May leverage its capabilities in support of civilian emergencies under Defense Support of Civil Authorities.<br>▪ May support civil authorities for cyber incidents outside the DOD Information Network (DODIN) under Defense Support for Cyber Incident Response when requested by one of the federal lead agencies under PPD-41 and approved by DOD, or directed by the President—with support provided based on the needs of the incident, capabilities required, readiness of available forces, and evaluation of resource needs for other DOD missions.<br>▪ Disseminates cyber threat reports and mitigations relevant to the defense industrial base through various channels, including the National Security Agency (NSA) and the DOD Cyber Crime Center (DC3). |
| **Federal Bureau of Investigation** | ▪ Coordinates with CISA to ensure unity of effort between threat and asset response activities. |

[16] 6 USC §677b et seq. The Cyber Response and Recovery Fund is a CISA-administered fund which can be used for certain coordination activities, response and recovery support related to specific significant incidents declared under the Cyber Response and Recovery Act; for certain advance activities authorized by statute; and for certain grants and cooperative agreements. Use of the fund is subject to several specific requirements in the Cyber Response and Recovery Act, including a significant incident declaration by the Secretary of Homeland Security in coordination with the National Cyber Director based on a finding that the incident is a significant incident and that otherwise available resources are insufficient to effectively respond to or mitigate the incident.

| Entity | Role(s) In Asset Response |
|---|---|
| SRMAs | ▪ Maintain and provide situational awareness on threats, incidents, or events impacting critical infrastructure as appropriate and to facilitate information sharing within respective sectors.<br>▪ Support, in coordination with CISA, incident management and restoration efforts during or following a security incident.<br>▪ Support CISA, upon request, in asset response efforts within the sector, leveraging domain-specific technical knowledge and capabilities as feasible.[17] |
| Other Federal and SLTT Government Responders | ▪ May activate their own asset response capabilities and cyber incident response plans to support cyber incidents in their jurisdiction.<br>▪ The National Guard may provide direct support under Title 32 to state-level response under direction of the state's governor.<br>▪ Fusion Centers may produce and disseminate locally relevant cybersecurity information and to serve as a coordination point for federal and local cybersecurity analysts. |
| Information Sharing and Analysis Center (ISAC) and Information Sharing and Analysis Organization (ISAO) | ▪ Facilitate information sharing among members and partners.<br>▪ May assist members in incident response and remediation, threat analysis, and early warning notifications. |
| Non-Federal Affected Entities | ▪ Primarily responsible for leading, executing, and resourcing their response under applicable laws and regulations.<br>▪ May report and share information regarding cyber incidents and malicious cyber activity to appropriate federal entities.<br>▪ Voluntarily participate in collaborative efforts to:<br>○ Understand and evaluate the impact of an incident through CISA, ISACs, SRMAs, or other entities.<br>○ Respond to and recover from cyber incidents through CISA, ISACs, SRMAs, or other entities. |
| Federal Civilian Executive Branch Affected Entity | ▪ Primarily responsible for leading, executing, and resourcing their response under applicable laws and regulations.<br>▪ Work with CISA to identify, respond to, and recover from cyber incidents, including complying with Emergency Directives and other CISA guidance. |
| Non-Affected Entities | ▪ Review information on evolving cyber incidents, including alerts and advisories, to reassess risk and implement additional security measures as appropriate. |

[17] Section 665d of title 6, United States Code, sets forth SRMA responsibilities, which are further expanded on in NSM-22.

## Threat Response

**PPD-41 Description**: Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.[18]

**Federal LOE Lead Agency:** The DOJ/FBI, FBI-designated field offices, and NCIJTF are the primary law enforcement entities that develop and implement threat response. The U.S. Secret Service and other law enforcement entities will also investigate cybercrime and contribute to threat response as needed within their jurisdictions.[19]

**Stakeholders**: **Table 8** describes key stakeholders and their role in threat response.

***Table 8: Primary Entity Roles in Threat Response***

| Entity | Role(s) In Threat Response |
|---|---|
| Department of Justice | ▪ Prosecutes federal cases arising from cyber incident investigations.<br>▪ Along with other federal law enforcement entities, disrupt criminal and national security cyber threats through any other means within their authority. |
| Federal Bureau of Investigation | ▪ Primarily leads threat response activities.<br>▪ Investigates, attributes, and disrupts malicious cyber activity.<br>▪ Can provide cyber threat information, experts, and capabilities to inform response efforts.<br>▪ Can provide decryption capabilities or other known mitigation tools, if available.<br>▪ Assists in freezing, seizing, and returning stolen and extorted funds, when possible.<br>▪ Notifies entities who may be unaware they have been compromised, in coordination with other federal entities, as appropriate. |

[18] Threat and asset responders will share some responsibilities and activities, which may include communicating with affected entities to understand the nature of the cyber incident; providing information to affected entities on available federal resources and capabilities; promptly disseminating through appropriate channels intelligence and information learned in the course of the response; and facilitating information sharing and operational coordination with other federal government entities.

[19] With support from other Federal agencies, as appropriate, US Cyber Command leads Threat Response for the Department of Defense Information Network and the Intelligence Community (IC) Security Coordination Center leads Threat Response for the IC Information Environment.

| | |
|---|---|
| Law Enforcement Entities | ▪ Investigate computer intrusions and contribute to threat response as needed.<br>▪ Federal law enforcement entities collaborate closely with other federal, SLTT, and international law enforcement, along with public and private sector partners, to investigate illicit cyber activity.<br>▪ State and local law enforcement entities, sometimes in coordination with federal law enforcement, investigate violations of state and local criminal statutes against unauthorized access or damage to computer systems, and incident reporting in regulated sectors.<br>▪ Fusion centers are situated at the intersection between federal and SLTT law enforcement and facilitate coordination among threat responders from different jurisdictions. |
| Department of Defense | ▪ Responds to cyber incidents affecting the DODIN and DIB entities.<br>▪ May, under specific circumstances identified in law and in coordination with civil authorities, assist in identifying and defending against cyber threats originating outside the United States through USCYBERCOM.<br>▪ May provide additional support to cyber incident responses under various legal authorities, including the Defense Support to Civil Authorities process. |
| CISA | ▪ Disseminates information learned during asset response to threat responders through appropriate channels.<br>▪ Notifies entities who may be unaware they have been compromised, in coordination with other federal entities as appropriate. |
| SRMAs | ▪ Assist in threat response by identifying and notifying similarly postured entities within a sector of emerging or known threats.<br>▪ Support threat response with technical capabilities, as appropriate and requested.<br>▪ Provide additional context based on sector-specific expertise and insight. |
| Private Sector | ▪ May report and share information regarding cyber incidents and malicious cyber activity to appropriate federal entities. |

## Intelligence Support

**PPD-41 Description**: Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.

**Federal LOE Lead Agency:** The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, will lead coordinated intelligence support in response to a cyber incident.

377 **Stakeholders: Table 9** describes key stakeholders and their role in intelligence support.

*Table 9. Primary Entity Roles in Intelligence Support*

| Entity | Role(s) In Intelligence Support |
|---|---|
| Office of the Director of National Intelligence (ODNI) | ▪ Facilitates the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.<br>▪ Provides threat reporting at levels of classification appropriate to the circumstances and demands of the incident, to include seeking declassification and/or downgraded reports.<br>▪ Coordinates any intelligence collection, analysis, and production activities that may take place as part of the incident through the National Intelligence Manager for Cyber. |
| CISA | ▪ Serves as the primary federal civilian interface for developing and sharing information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for federal and non-federal entities.<br>▪ Coordinates the sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents across the federal government. |
| SRMAs | ▪ Facilitating, in coordination with CISA, access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure,<br>▪ Facilitating awareness within the designated sector or subsector of such sector, of ongoing, and where possible, real-time awareness of identified threats, vulnerabilities, mitigations, and other actions related to the security of such sector or subsector of such sector.<br>▪ Facilitating the identification of intelligence needs and priorities of critical infrastructure owners and operators in the designated sector or subsector of such sector, in coordination with the Director of National Intelligence and the heads of other Federal departments and agencies, as appropriate. |
| DOJ/FBI | ▪ Provides sharable intelligence gathered through threat response activities. |
| All IC Components | ▪ Provides intelligence support as requested under ODNI coordination. |

## Affected Entity Response

378 **PPD-41 Description:** An affected federal department or agency's efforts to manage the impact of a
379 cyber incident, which may include maintaining business or operational continuity; 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.

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 established in PPD-41, and in coordination with the affected entity.

**Federal LOE Lead Agency:** When a cyber incident affects federal departments or agencies, each affected department or agency is responsible for leading and resourcing its own cyber incident response in coordination with CISA; or in the case of DOD or IC entities, USCYBERCOM or the IC SCC, respectively.

Summary of Federal Civilian Executive Branch Entity Roles and Responsibilities:

- CISA leads asset response for the FCEB, while the affected FCEB entity has the primary responsibility for executing and resourcing a response.[20]
- Affected FCEB entities must report incidents potentially compromising the confidentiality, integrity, or availability of a federal information system to CISA.
- The affected department or agency may request assistance from CISA and other government agencies.
- The affected department or agency shall support law enforcement investigation of the incident.
- The affected department or agency shall implement directives to mitigate cybersecurity risk and vulnerabilities issued by the cognizant agency (CISA for FCEB entities, USCYBERCOM for DODIN and the DIB, and the IC SCC for the IC).
- The affected department or agency may be invited or directed to participate in a UCG and/or the CRG, even if not ordinarily a member of the CRG.

The affected federal entity may have additional obligations under applicable contracts or legal instruments.

DOD and IC entities should consult guidance provided by USCYBERCOM or the IC SCC for further information on their affected entity response roles and responsibilities.

[20] FCEB operational procedures are covered in detail in the Federal Government Cybersecurity Incident and Vulnerability Response Playbooks.

# Annex E: Follow-On Implementation Activities

This NCIRP provides a foundational framework for national coordination of cyber incident response. Further work is needed to fully implement this framework in operations across the national stakeholder community. **Table 10** lists follow-on activities that can help more fully realize implementation of the NCIRP.

***Table 10. Follow-On Implementation Activities***

| Enabling Capability | Purpose | Responsibility |
|---|---|---|
| Cyber UCG Concept of Operations | Provide direction for unified national cyber incident coordination, including stand-up, participation, and process. | PPD-41 LOE Leads |
| Asset Response Concept of Operations | Provide direction for federal, SLTT, and private sector cyber incident coordination in the asset response LOE, including how JCDC will be leveraged to coordinate across federal and non-federal stakeholders, and how incident-specific working groups will form and operate. | CISA |
| Cyber Incident Severity Scoring Process | National process to evaluate and score the severity of incidents relative to the Cyber Incident Severity Schema. | PPD-41 LOE Leads |
| National Incident Management System and Incident Command System Integration | Establishes common doctrine and practice for cyber and all-hazards response to enhance unity of effort. | CISA, Federal Emergency Management Agency |
| Sector and SLTT-Specific NCIRP Implementation Plans | Generate guidance tailored to critical infrastructure providers that tailors NCIRP processes to specific sectors and SLTT jurisdictions. | CISA, SRMAs, ISACs, SLTT governments |
| Designated NCIRP Personnel/Offices | Assign personnel and facilities to support Cyber UCG and LOE functional requirements. | Cyber UCG Core Participants |
| NCIRP Participant Training | Ensure personnel who may be involved with NCIRP responses understand their role in the process and are prepared for effective coordination in advance of incidents. | Cyber UCG, LOE Participants |

| | | |
|---|---|---|
| NCIRP Table-Top Exercises | Train public and private participants on roles, responsibilities, decisions, and actions during an incident requiring federal coordination; test and improve the incident response plan. | CISA |
| Public Information Plan Template | A predefined plan template for sharing information with stakeholders and the public during an incident that can be tailored to the specific circumstances of the incident. | CISA |
| Communication Tools | Tools and platforms for effective communication during an incident, such as secure messaging apps and conference call systems. | CISA |
| Memorandums of Understanding and/or Information Sharing Agreements with Cyber Incident Response Partners | Speed participation and flow of information across necessary stakeholders during an incident. | CISA, Private Sector, and International Partners |

# Annex F: Additional Resources

The following links provide additional cybersecurity incident response and sector-specific resources.

- **National Institute of Standards and Technology**
  - Incident Response, Overview
  - Incident Response, Preparation Resources
  - Incident Response, Life Cycle Resources
- **Cybersecurity and Infrastructure Security Agency**
  - Incident Response Plan (IRP) Basics (cisa.gov)
  - Free Cybersecurity Services & Tools | CISA
- **Information Sharing and Analysis Centers**
  - National Council of ISACs - Member ISACs
- **Information Sharing and Analysis Organization Standards Organization**
  - Information Sharing Groups Browser – ISAO Standards Organization
- **Cybersecurity resources for U.S. State, Local, Tribal, and Territorial (SLTT) government organizations**
  - CISA resources for SLTT Governments
  - Multi-State ISAC
  - Elections Infrastructure ISAC
  - Tribal ISAC
- **Sector Specific Resources**
  - Chemical Sector: Chemical Sector Cybersecurity Resources
  - Commercial Facilities Sector: Commercial Facilities Sector Cybersecurity Framework Implementation Guidance | CISA – Media+Entertainment ISAC – Real Estate ISAC – Retail and Hospitality ISAC
  - Communications Sector: Communications and Cyber Resiliency Toolkit | CISA and Network Reliability Resources | Federal Communications Commission (fcc.gov) – Communications ISAC – Small Broadband Provider ISAC
  - Critical Manufacturing Sector: Critical Cybersecurity Manufacturing Sector Resources
  - Dams Sector: Dams Sector Cybersecurity Capability Maturity Model (C2M2) 2022 | CISA
  - Defense Industrial Base Sector: Defense Industrial Base (DIB) Cybersecurity Portal (dod.mil) – National Defense ISAC
  - Emergency Services Sector: Emergency Services Cybersecurity Initiative – Emergency Management and Response ISAC
  - Energy Sector: Cybersecurity | Department of Energy – Downstream Natural Gas ISAC – Electricity ISAC – Oil and Natural Gas ISAC
  - Financial Services Sector: Financial Institutions | U.S. Department of the Treasury - FDIC Cybersecurity Resources – Financial Services ISAC

- Food and Agriculture Sector: Food and Ag ISAC
- Government Services and Facilities Sector: Research and Education Networks ISAC
- Health and Public Health Sector: HC3 Products | HHS.gov – Health ISAC
- Information Technology Sector: IT-ISAC
- Nuclear Reactors, Materials, and Waste Sector: Nuclear Sector Cybersecurity Framework Implementation Guidance | CISA and US Nuclear Regulatory Commission Cybersecurity Resources
- Transportation Systems Sector: Department of Transportation Cybersecurity Resources and Cybersecurity Resources for Transit Agencies | FTA (dot.gov) – Automotive ISAC – Aviation ISAC – Maritime ISAC – Maritime Transportation System ISAC – Surface Transportation, Public Transportation, and Over-the-Road Bus ISACs
- Water and Wastewater Systems Sector: EPA Cybersecurity for the Water Sector | US EPA – Water ISAC

- **Multi Sector Resources**
  - Space ISAC

# Annex G: Authorities and Statutes

The authorities listed below summarize key legal and policy authorities related to cyber incident response activities involving federal coordination. This list is not exhaustive but is provided for reference only.

- **Homeland Security, Resilience, and Emergency Response**
  - Cybersecurity and Infrastructure Security Agency Act of 2018
  - Homeland Security Act of 2002, as amended
  - Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended
  - EO 13618: Assignment of National Security and Emergency Preparedness Communications Functions
  - PPD-8: National Preparedness
  - NSM-22: Critical Infrastructure Security and Resilience
  - PPD-40: National Continuity Policy
  - PPD-41: U.S. Cyber Incident Coordination Policy, and its accompanying Annex
  - HSPD-5: Management of Domestic Incidents
- **Information and Communication Technology**
  - Title 47-Telecommunications
  - Cyber Incident Reporting for Critical Infrastructure Act of 2022
  - Communications Act of 1934, Section 706
  - Cybersecurity Act of 2015
  - National Cybersecurity Protection Act of 2014
  - EO 13636: Improving Critical Infrastructure Cybersecurity
  - EO 13691: Promoting Private Sector Cybersecurity Information Sharing
  - EO 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
  - EO 14028: Improving the Nation's Cybersecurity
  - National Security Memorandum (NSM) 5: Improving Cybersecurity for Critical Infrastructure Control Systems
  - National Cybersecurity Strategy of 2023
- **Federal Information and Communication Technology Systems**
  - Federal Information Security Modernization Act of 2014
  - National Security Directive 42: National Policy for the Security of National Security Telecommunications and Information Systems
  - NSPD-54/HSPD-23: Cybersecurity Policy
  - NSM 8: Improving the Cybersecurity of National Security, Department of Defense (DoD), and Intelligence Community Systems

- OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
- OMB M-21-31 Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

- **Federal Statutory Mechanisms for Prosecuting Cybercrime**
  - Computer Fraud and Abuse Act (CFAA)
  - Stored Communications Act
  - Economic Espionage Act of 1996, as amended by the Defend Trade Secrets Act of 2016
  - Wire Fraud statute
- **National Security, Intelligence, and Law Enforcement**
  - Title 6 – Domestic Security
  - Title 10 – Armed Forces
  - Title 18 – Crimes and Criminal Procedure
  - Title 32 – National Guard
  - Title 50 – War and National Defense
  - Intelligence Reform and Terrorism Prevention Act of 2004
  - National Security Act of 1947, as amended
  - EO 12333: United States Intelligence Activities, 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 12829: National Industrial Security Program, as amended
  - Secretary of Defense Memorandum, "Delegation of Authority to Make Arrangements with Private Sector Entities Pursuant to Section 1642(b) of the National Defense Authorization Act for Fiscal Year 2019," dated 1 October 2022
- **Additional authorities in times of a national emergency declared by the President or Congress, a declaration of war, and other situations in which a state of war may exist absent a declaration of war:**
  - 10 USC §12301 et seq. governing the activation of reserve forces
  - Defense Production Act of 1950, as amended
  - 47 USC §606 War powers of the President

# Annex H: Acronym List

| Acronym | Definition |
|---|---|
| C2M2 | Cybersecurity Capability Maturity Model |
| CFAA | Computer Fraud and Abuse Act |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CRG | Cyber Response Group |
| CRRF | Cyber Response and Recovery Fund |
| CSA | Cybersecurity Advisor |
| CTIIC | [ODNI] Cyber Threat Intelligence Integration Center |
| Cyber UCG | Cyber Unified Coordination Group |
| DC3 | Department of Defense Cyber Crime Center |
| DHS | Department of Homeland Security |
| DIB | Defense Industrial Base |
| DOD | Department of Defense |
| DODIN | Department of Defense Information Network |
| DOJ | Department of Justice |
| EO | Executive Order |
| EPA | Environmental Protection Agency |
| FBI | Federal Bureau of Investigation |
| FCEB | Federal Civilian Executive Branch |
| FDIC | Federal Deposit Insurance Corporation |
| FTA | Federal Transportation Administration |
| HC3 | Health Sector Cybersecurity Coordination Center |
| HSPD-5 | Homeland Security Presidential Directive 5 |

| | |
|---|---|
| IC | Intelligence Community |
| IC SCC | [ODNI] Intelligence Community Security Coordination Center |
| IRP | Incident Response Plan |
| ISAC | Information Sharing and Analysis Center |
| ISAO | Information Sharing and Analysis Organization |
| IT | Information Technology |
| JCDC | Joint Cyber Defense Collaborative |
| LE | Law Enforcement |
| LOE | Lines of Effort |
| NCIJTF | National Cyber Investigative Joint Task Force |
| NCIRP | National Cyber Incident Response Plan |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NSC | National Security Council |
| NSM | National Security Memorandum |
| NSPD | National Security Presidential Directive |
| ODNI | Office of the Director of National Intelligence |
| OMB | Office of Management and Budget |
| PPD | Presidential Policy Directive |
| PPD-41 | Presidential Policy Directive 41 – U.S. Cyber Incident Coordination |
| SLTT | State, Local, Tribal, and Territorial |
| SRMA | Sector Risk Management Agency |
| UCG | [National Response Framework] Unified Coordination Group |
| USC | U.S. Code |

| | |
|---|---|
| USCYBERCOM | United States Cyber Command |