



# 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**

*This document is distributed as TLP:CLEAR. Recipients may share TLP:CLEAR information without restriction. Subject to standard copyright rules. For more information on the Traffic Light Protocol, see [cisa.gov/tlp](https://cisa.gov/tlp).*

## Contents

Executive Summary .....	3
Introduction.....	4
Lines of Effort.....	5
Coordinating Structures.....	7
Phases of Cyber Incident Response Operations.....	10
Detection Phase.....	11
Response Phase.....	14
Post-Incident Activities.....	20
Implementation and Maintenance .....	20
CISA Activities.....	20
Federal Departments and Agencies.....	21
Nationwide Activities .....	21
Conclusion .....	21
Annex A: Cyber Incident Severity Schema .....	22
Annex B: Preparing for Cyber Incidents .....	23
Annex C: Voluntary Reporting of Cyber Incidents to the Federal Government .....	25
Annex D: Stakeholder Roles and Responsibilities by Line of Effort.....	27
Asset Response .....	27
Threat Response.....	30
Intelligence Support.....	31
Affected Entity Response .....	32
Annex E: Follow-On Implementation Activities.....	34
Annex F: Additional Resources .....	36
Annex G: Authorities and Statutes .....	38
Annex H: Acronym List .....	40

## Executive Summary

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

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

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

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

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

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

## Introduction

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

---

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

45 *CISA Director Jen Easterly*  
46 *Before the House Select Committee on Strategic Competition Between the*  
47 *United States and the Chinese Communist Party*  
48 *January 31, 2024*  
49

---

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

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

---

<sup>1</sup> 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.

<sup>2</sup> Cybersecurity plans. 6 USC §660(c) and (d)

67 [Presidential Directive 5 \(HSPD-5\)–Management of Domestic Incidents](#) or other federal or non-  
 68 federal authorities. To integrate cyber and physical incident response per PPD-41, the NCIRP  
 69 leverages doctrine from the Federal Emergency Management Agency’s National Response  
 70 Framework, the National Incident Management System, and the Incident Command System.

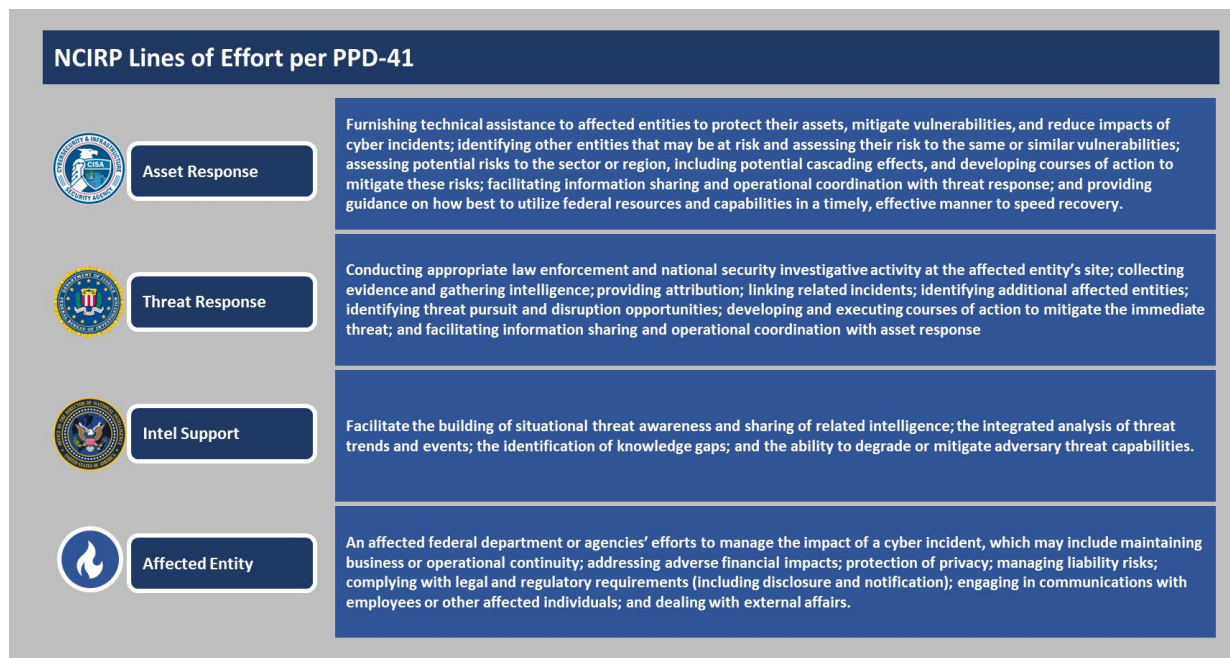
**Table 1: Cyber Incident Definitions from PPD-41**

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. <sup>3</sup>

## Lines of Effort

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

<sup>3</sup> 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**

75 The leads for each LOE are:

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

<sup>4</sup> 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.

<sup>5</sup> 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.

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

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

## Coordinating Structures

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

107 **Table 2** provides a summary of the existing coordinating structures that may be involved in cyber  
 108 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
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: <ul style="list-style-type: none"> <li>▪ Receiving updates from federal agencies and measures being taken to resolve or respond</li> <li>▪ Resolving issues elevated to it by subordinate bodies such as the Cyber UCG</li> <li>▪ Collaborating with other groups in the National Security Council (NSC) when a cross-disciplinary response is required</li> </ul>

Name	Coordinating Lead Organization	Purpose in Cyber Incident
		<ul style="list-style-type: none"> <li>▪ Identifying and considering options for response and making recommendations to the Deputies Committee when higher level guidance is required</li> <li>▪ Considering the policy implications for public messaging</li> <li>▪ Coordinating a communications strategy as necessary</li> </ul>
Cyber Unified Coordination	<p>Participation will regularly</p> <ul style="list-style-type: none"> <li>▪ CISA, FBI, CTIC as LOE leads</li> <li>▪ SRMAs for affected critical infrastructure sectors</li> <li>▪ Affected federal departments or agencies</li> <li>▪ Other responding federal agencies</li> </ul> <p>May include non-federal participation in limited circumstances.</p> <p>CISA may serve as an executive secretariat for the Cyber UCG to support its operations.</p>	<p>Per PPD-41, the Cyber UCG 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.</p>



Name	Coordinating Lead Organization	Purpose in Cyber Incident
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. <sup>6</sup>

---

<sup>6</sup> 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.  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

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

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

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

### Detection Phase

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

131 **Key Decisions and Activities:** **Table 3** outlines key decisions that could be made during the detection  
 132 phase of a cyber incident, as well as the coordinating structure(s) associated with the decision.

133 **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	<ul style="list-style-type: none"> <li>▪ Informs level of effort and resource commitments needed</li> <li>▪ May inform significant incident declaration process under the Cyber Response and Recovery Act</li> </ul>	<ul style="list-style-type: none"> <li>▪ Impact to the nation</li> <li>▪ Threat intelligence</li> <li>▪ Geopolitical context</li> <li>▪ SRMA domain expertise</li> </ul>	<p>Consensus of CRG agencies.</p> <p>NSC when CRG agencies disagree</p>

Key Decision	Why It Matters	Information Supporting Decision	Decision Mechanism
<p>Determine if CISA should convene an incident-specific group of stakeholders through the JCDC to coordinate asset response activities across stakeholders</p>	<ul style="list-style-type: none"> <li>▪ Creates a scalable and predictable structure for the detection, and if needed, response processes</li> <li>▪ Promotes unity of effort across public and private sectors</li> </ul>	<ul style="list-style-type: none"> <li>▪ Input from stakeholders collaborating on detection and analysis</li> <li>▪ Number and criticality of stakeholders involved</li> </ul>	<p>CISA in collaboration with other detection and response stakeholders</p>
<p>Determine if a Cyber UCG, or other coordinating mechanism, is needed</p>	<ul style="list-style-type: none"> <li>▪ Identifies a need for greater coordination between agencies exercising their existing authorities in response to an incident</li> <li>▪ Requires executive-level engagement from responding federal agencies, including SRMAs</li> <li>▪ Promotes governmental unity of effort with respect to incident response</li> </ul>	<ul style="list-style-type: none"> <li>▪ Severity of incident</li> <li>▪ Scale of incident</li> <li>▪ Complexity of coordination needed</li> <li>▪ Number of agencies involved</li> </ul>	<p>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)<sup>7</sup></p>

<sup>7</sup> 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	<ul style="list-style-type: none"> <li>▪ CISA, leveraging the JCDC</li> <li>▪ SRMAs</li> </ul>	<ul style="list-style-type: none"> <li>▪ Leverage private sector information and expertise in assessing scale and scope of incident</li> </ul>	<ul style="list-style-type: none"> <li>▪ Increased comprehensive situational awareness about the incident</li> </ul>
Identify and acquire priority information needs	<ul style="list-style-type: none"> <li>▪ CISA</li> <li>▪ DOJ/FBI</li> <li>▪ ODNI</li> <li>▪ SRMAs</li> <li>▪ Other stakeholders participating in response</li> </ul>	<ul style="list-style-type: none"> <li>▪ Focus information gathering, information sharing, and intelligence efforts</li> </ul>	<ul style="list-style-type: none"> <li>▪ Develop the information needed for collaborative analysis to understand the scale, scope, and impact of the cyber incident</li> </ul>
Conduct collaborative risk and impact assessment and share results	<ul style="list-style-type: none"> <li>▪ CISA</li> <li>▪ SRMAs</li> <li>▪ DOJ/FBI</li> <li>▪ ODNI</li> </ul>	<ul style="list-style-type: none"> <li>▪ Leverage and share the insights and analytical capabilities available across the stakeholder community</li> </ul>	<ul style="list-style-type: none"> <li>▪ Form a unified and comprehensive as possible picture of the nature, scale, scope, and impact of the incident</li> <li>▪ Support attribution</li> </ul>

<p>Understand scope and impact of incident</p>	<ul style="list-style-type: none"> <li>▪ CISA</li> <li>▪ DOJ/FBI</li> <li>▪ ODNI</li> <li>▪ SRMAs</li> <li>▪ Responding ISACs/ISAOs</li> <li>▪ Relevant Vendors</li> <li>▪ Other stakeholders with high visibility into affected portions of ecosystem (e.g., Internet Service Providers, managed service providers, cloud providers)</li> </ul>	<ul style="list-style-type: none"> <li>▪ For major incidents, no one stakeholder has a comprehensive view</li> <li>▪ Insights of multiple stakeholders usually needed to form a complete and accurate picture of an incident and its impacts</li> </ul>	<ul style="list-style-type: none"> <li>▪ 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</li> <li>▪ Understand cross-sector impacts and risks</li> </ul>
--	--	---	--

### Response Phase

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

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

*Table 5. Key Decisions-Response Phase*

Key Decision	Why It Matters	Information Supporting Decision	Decision Mechanism
<p>Determine key non-governmental stakeholders to contribute to solution development and implementation</p>	<ul style="list-style-type: none"> <li>▪ Identifies the technical expertise and services that are available in the private sector</li> </ul>	<ul style="list-style-type: none"> <li>▪ Relevant technical expertise and reach</li> <li>▪ Likelihood of effectiveness</li> </ul>	<ul style="list-style-type: none"> <li>▪ CISA in coordination with the CRG/Cyber UCG, other LOE leads and SRMAs</li> </ul>

<p>Determine shared priorities for response</p>	<ul style="list-style-type: none"> <li>Promotes unity of effort across stakeholders</li> <li>Ensures most important activities are the focus</li> </ul>	<ul style="list-style-type: none"> <li>Scope and impact of incident</li> <li>Response options and resources available</li> <li>National leadership priorities</li> <li>Overall context of the situation</li> </ul>	<ul style="list-style-type: none"> <li>Cyber UCG</li> </ul>
<p>Determine when and how to implement response activities</p>	<ul style="list-style-type: none"> <li>Promotes unity of effort and deconfliction coordination</li> <li>Synchronizes response activities for maximum effectiveness</li> </ul>	<ul style="list-style-type: none"> <li>Capabilities stakeholders have and when they can be implemented</li> <li>Understanding of incident dynamics</li> </ul>	<ul style="list-style-type: none"> <li>LOE leads in coordination with one another, and when activated, the Cyber UCG</li> </ul>
<p>Determine whether otherwise available resources, other than the Cyber Response and Recovery Fund (CRRF), are likely insufficient to effectively respond or mitigate the incident</p>	<ul style="list-style-type: none"> <li>Resource insufficiency is one of the requirements for a significant incident declaration and access to the CRRF</li> <li>The CRRF can provide additional resources to support incident response if otherwise available resources are insufficient</li> </ul>	<ul style="list-style-type: none"> <li>Assessment of the requirements for incident response and comparison with available resources</li> </ul>	<ul style="list-style-type: none"> <li>CISA coordinates requests for Secretary of DHS determination in consultation with the National Cyber Director</li> </ul>
<p>Determine conditions for ending the incident response phase</p>	<ul style="list-style-type: none"> <li>Indicates federal response coordination is no longer needed</li> </ul>	<ul style="list-style-type: none"> <li>Effectiveness of response activities</li> <li>Full scope of incident</li> <li>Status of incident response stakeholder capabilities and operational state</li> </ul>	<ul style="list-style-type: none"> <li>LOE leads in coordination with one another, or when activated, the Cyber UCG</li> </ul>

Table 6. Coordinated Activities-Response Phase

Coordinated Activity	Core Participants	Why Coordinate	Intended Outcome of
<p>Identify information and support needs of the affected entities and other key stakeholders</p>	<ul style="list-style-type: none"> <li>▪ CISA</li> <li>▪ DOJ/FBI</li> <li>▪ ODNI</li> <li>▪ SRMAs</li> </ul>	<ul style="list-style-type: none"> <li>▪ Establish lines of communication</li> <li>▪ Enable information sharing, containment, and further detection and response actions</li> <li>▪ Prioritize LOE activities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Affected entities and other key stakeholders are able to communicate and collaborate with appropriate federal agencies</li> <li>▪ Federal engagement with affected entities occurs in a coordinated way</li> </ul>
<p>Develop initial options and priorities</p>	<ul style="list-style-type: none"> <li>▪ CISA coordinates 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</li> </ul>	<ul style="list-style-type: none"> <li>▪ Better understand incident and support immediate containment activities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Reduced risk of</li> <li>▪ Set conditions for further remediation</li> </ul>
<p>Develop strategy for implementing, synchronizing, and measuring the effectiveness of response activities</p>	<ul style="list-style-type: none"> <li>▪ CISA</li> <li>▪ DOJ/FBI</li> <li>▪ ODNI</li> <li>▪ SRMAs</li> <li>▪ Other relevant stakeholders as determined by LOE leads</li> </ul>	<ul style="list-style-type: none"> <li>▪ Transition from immediate containment to more comprehensive response</li> <li>▪ Identify initial measures of effectiveness for different response activities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Nationally coordinated incident response effort</li> <li>▪ Facilitates transition from detection phase to response phase</li> </ul>



<p>Develop mitigation</p>	<ul style="list-style-type: none"> <li>▪ CISA, DOJ/FBI, other federal agencies with relevant expertise</li> <li>▪ Responding ISACs/ISAOs</li> <li>▪ Relevant product vendors</li> <li>▪ Incident response firms/teams</li> <li>▪ Other technically capable affected or at-risk entities</li> </ul>	<ul style="list-style-type: none"> <li>▪ There are often mitigate an incident, and different stakeholders may identify differing approaches</li> <li>▪ Initial mitigation guidance is often improved upon by others</li> </ul>	<ul style="list-style-type: none"> <li>▪ Mitigation developed, validated, and published</li> </ul>
<p>Publish and amplify mitigation guidance</p>	<ul style="list-style-type: none"> <li>▪ CISA, DOJ/FBI, ODNI, SRMAs, and other federal agencies with relevant expertise</li> <li>▪ Responding ISACs/ISAOs</li> <li>▪ Relevant product vendors</li> <li>▪ Private sector incident response firms/teams</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ensure accurate and consistent guidance is available across multiple communications channels</li> <li>▪ Maximize speed and reach of publication by leveraging the communications channels and audiences available to different stakeholders</li> </ul>	<ul style="list-style-type: none"> <li>▪ Mitigation guidance is widely available from trustworthy sources</li> </ul>
<p>Information sharing coordination with international government partners</p>	<ul style="list-style-type: none"> <li>▪ CISA</li> <li>State</li> <li>▪ DOJ/FBI</li> <li>▪ ODNI</li> <li>▪ SRMAs</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ensure messaging across U.S. government agencies</li> <li>▪ Leverage all relevant partnerships available across the U.S. government</li> </ul>	<ul style="list-style-type: none"> <li>▪ All relevant effectively engaged for an incident</li> </ul>

		<ul style="list-style-type: none"> <li>Ensure unity of international partners</li> </ul>	
Investigate and identify perpetrating threat actors	<ul style="list-style-type: none"> <li>DOJ/FBI</li> <li>Other law enforcement</li> <li>CISA</li> <li>ODNI</li> <li>SRMAs</li> </ul>	<ul style="list-style-type: none"> <li>Information gained through asset response or intelligence activities may contribute to threat response</li> <li>Information gained in investigation may be relevant to other lines of effort</li> </ul>	<ul style="list-style-type: none"> <li>Law enforcement can identify and further pursue and/or prosecute perpetrating threat actors</li> </ul>
Disrupt threat actors	<ul style="list-style-type: none"> <li>DOJ/FBI</li> <li>enforcement</li> <li>DOD</li> <li>ODNI</li> <li>CISA</li> <li>Technology ecosystem companies or other non-governmental entities, as appropriate</li> </ul>	<ul style="list-style-type: none"> <li>Various U.S. agencies have capabilities relevant to disrupting threat actor activity</li> <li>At times, technology ecosystem companies or other non-governmental stakeholders may have relevant capabilities to disrupt threat actors</li> </ul>	<ul style="list-style-type: none"> <li>Threat actor degraded or destroyed</li> </ul>

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

- 147
  - Contributing to prioritization and adjudication of response options across the LOEs
- 148
  - Working to restore critical services as quickly as possible

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

151   **Coordination Considerations:**

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

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

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

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

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

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

182   Enhanced coordination procedures help to:

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

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

## Post-Incident Activities

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

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

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

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

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

## Implementation and Maintenance

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

## CISA Activities

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

---

<sup>8</sup> PPD-41 Annex at IV(E)

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

220 CISA has statutory responsibility to update, maintain, and exercise the NCIRP.<sup>10</sup> The updates will  
221 keep the NCIRP current with changes in the cyber threat and cyber defense environment, changes  
222 in law and policy, and lessons learned from past incidents.

## Federal Departments and Agencies

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

## Nationwide Activities

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

## Conclusion

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

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

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

---

<sup>10</sup> Cybersecurity plans. 6 USC §660(c) and (d).

## Annex A: Cyber Incident Severity Schema

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

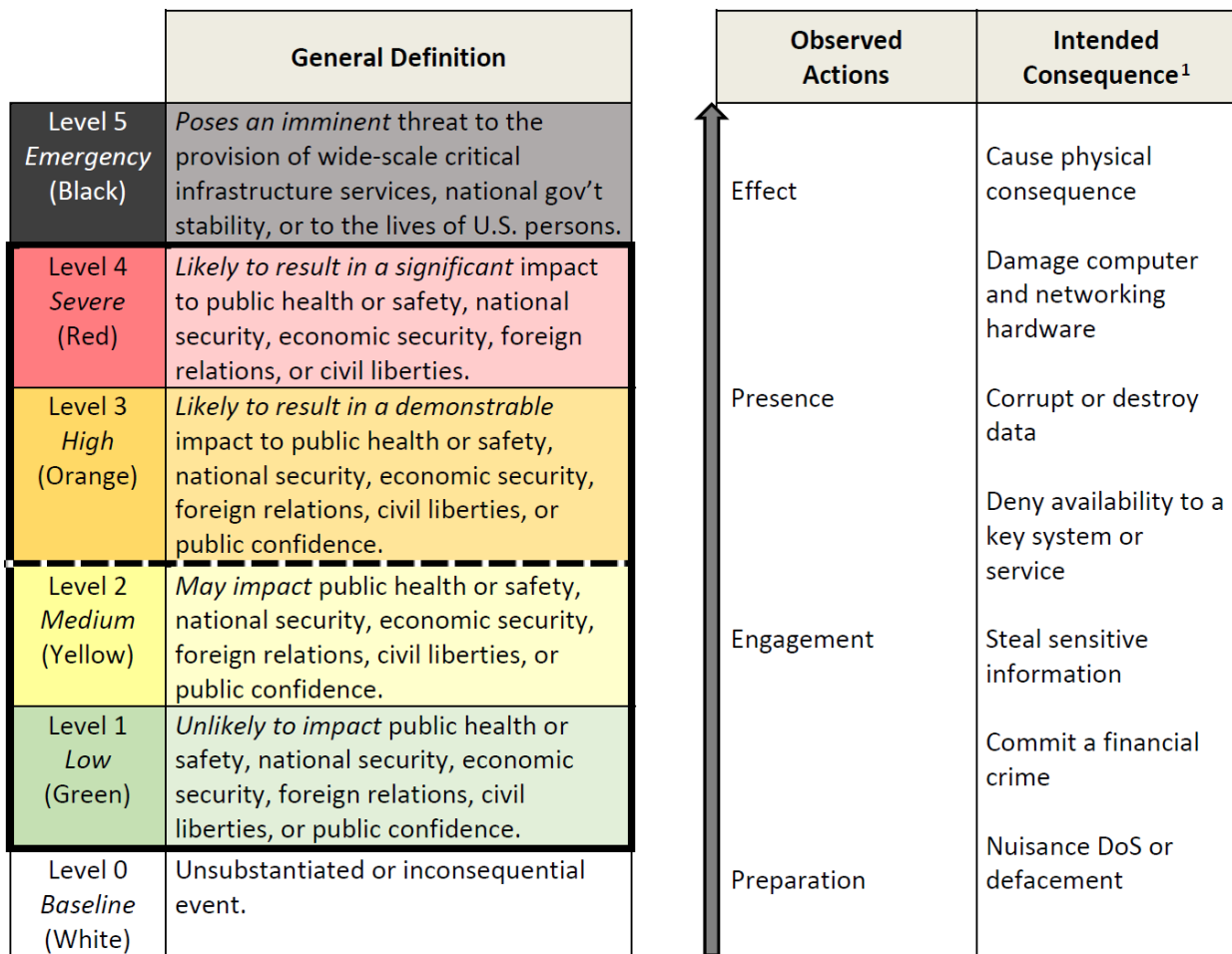


Figure 2: Cyber Incident Severity Schema

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

## Annex B: Preparing for Cyber Incidents

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

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

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

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

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

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

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

291 

- How to report?

- 292
  - Report incidents to CISA via its [web portal](#), [email](#), or by calling 1-844-SAY-CISA.
  - 293
    - Reports criminal incidents to the FBI via its [web portal](#) or by contacting an FBI field  
294 office.
    - 295
      - Reports of cyber-enabled financial crimes may be reported to the Secret Service through  
296 the [nearest field office](#).

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

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

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

---

<sup>11</sup> 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>.

<sup>12</sup> NIST SP 800-61 <https://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

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

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

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

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

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

- 330     ▪ Web: <https://www.cisa.gov/report>
- 331     ▪ Email: [central@cisa.dhs.gov](mailto:central@cisa.dhs.gov)
- 332     ▪ Phone: (888) 282-0870

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

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

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

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

---

<sup>13</sup> 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>.

346 *US Secret Service*

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

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

### Asset Response

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

357 Federal LOE Lead Agency: CISA<sup>14</sup>

358 **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	<ul style="list-style-type: none"> <li>▪ Lead federal asset response activities.</li> <li>▪ 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.</li> <li>▪ Operational lead for Federal Civilian Executive Branch (FCEB) cybersecurity.</li> <li>▪ Provides unity of effort, leveraging the JCDC to bring together public and private sector asset response activities.</li> <li>▪ 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.<sup>15</sup></li> <li>▪ 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.</li> <li>▪ 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.</li> </ul>

<sup>14</sup> 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.

<sup>15</sup> CISA also serves as the SRMA for several sectors, and therefore also has SRMA responsibilities for those sectors.

Entity	Role(s) In Asset Response
	<ul style="list-style-type: none"> <li>▪ 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:                             <ul style="list-style-type: none"> <li>○ 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.</li> <li>○ Can use the Cyber Response and Recovery Fund to fund certain authorized activities.<sup>16</sup></li> </ul> </li> </ul>
<p><b>Department of Defense</b></p>	<ul style="list-style-type: none"> <li>▪ Supports CISA’s asset response activities including, as appropriate, providing technical assistance and sharing information to support incident mitigation.</li> <li>▪ Provides cybersecurity assistance to Defense Industrial Base (DIB) entities and service providers upon request through multiple DOD entities.</li> <li>▪ May leverage its capabilities in support of civilian emergencies under Defense Support of Civil Authorities.</li> <li>▪ 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.</li> <li>▪ 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).</li> </ul>
<p><b>Federal Bureau of Investigation</b></p>	<ul style="list-style-type: none"> <li>▪ Coordinates with CISA to ensure unity of effort between threat and asset response activities.</li> </ul>

<sup>16</sup> 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	<ul style="list-style-type: none"> <li>▪ Maintain and provide situational awareness on threats, incidents, or events impacting critical infrastructure as appropriate and to facilitate information sharing within respective sectors.</li> <li>▪ Support, in coordination with CISA, incident management and restoration efforts during or following a security incident.</li> <li>▪ Support CISA, upon request, in asset response efforts within the sector, leveraging domain-specific technical knowledge and capabilities as feasible.<sup>17</sup></li> </ul>
Other Federal and SLTT Government Responders	<ul style="list-style-type: none"> <li>▪ May activate their own asset response capabilities and cyber incident response plans to support cyber incidents in their jurisdiction.</li> <li>▪ The National Guard may provide direct support under Title 32 to state-level response under direction of the state's governor.</li> <li>▪ Fusion Centers may produce and disseminate locally relevant cybersecurity information and to serve as a coordination point for federal and local cybersecurity analysts.</li> </ul>
Information Sharing and Analysis Center (ISAC) and Information Sharing and Analysis Organization (ISAO)	<ul style="list-style-type: none"> <li>▪ Facilitate information sharing among members and partners.</li> <li>▪ May assist members in incident response and remediation, threat analysis, and early warning notifications.</li> </ul>
Non-Federal Affected Entities	<ul style="list-style-type: none"> <li>▪ Primarily responsible for leading, executing, and resourcing their response under applicable laws and regulations.</li> <li>▪ May report and share information regarding cyber incidents and malicious cyber activity to appropriate federal entities.</li> <li>▪ Voluntarily participate in collaborative efforts to: <ul style="list-style-type: none"> <li>○ Understand and evaluate the impact of an incident through CISA, ISACs, SRMAs, or other entities.</li> <li>○ Respond to and recover from cyber incidents through CISA, ISACs, SRMAs, or other entities.</li> </ul> </li> </ul>
Federal Civilian Executive Branch Affected Entity	<ul style="list-style-type: none"> <li>▪ Primarily responsible for leading, executing, and resourcing their response under applicable laws and regulations.</li> <li>▪ Work with CISA to identify, respond to, and recover from cyber incidents, including complying with Emergency Directives and other CISA guidance.</li> </ul>
Non-Affected Entities	<ul style="list-style-type: none"> <li>▪ Review information on evolving cyber incidents, including alerts and advisories, to reassess risk and implement additional security measures as appropriate.</li> </ul>

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

## Threat Response

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

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

369 **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	<ul style="list-style-type: none"> <li>▪ Prosecutes federal cases arising from cyber incident investigations.</li> <li>▪ Along with other federal law enforcement entities, disrupt criminal and national security cyber threats through any other means within their authority.</li> </ul>
Federal Bureau of Investigation	<ul style="list-style-type: none"> <li>▪ Primarily leads threat response activities.</li> <li>▪ Investigates, attributes, and disrupts malicious cyber activity.</li> <li>▪ Can provide cyber threat information, experts, and capabilities to inform response efforts.</li> <li>▪ Can provide decryption capabilities or other known mitigation tools, if available.</li> <li>▪ Assists in freezing, seizing, and returning stolen and extorted funds, when possible.</li> <li>▪ Notifies entities who may be unaware they have been compromised, in coordination with other federal entities, as appropriate.</li> </ul>

<sup>18</sup> 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.

<sup>19</sup> 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	<ul style="list-style-type: none"> <li>▪ Investigate computer intrusions and contribute to threat response as needed.</li> <li>▪ 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.</li> <li>▪ 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.</li> <li>▪ Fusion centers are situated at the intersection between federal and SLTT law enforcement and facilitate coordination among threat responders from different jurisdictions.</li> </ul>
Department of Defense	<ul style="list-style-type: none"> <li>▪ Responds to cyber incidents affecting the DODIN and DIB entities.</li> <li>▪ 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.</li> <li>▪ May provide additional support to cyber incident responses under various legal authorities, including the Defense Support to Civil Authorities process.</li> </ul>
CISA	<ul style="list-style-type: none"> <li>▪ Disseminates information learned during asset response to threat responders through appropriate channels.</li> <li>▪ Notifies entities who may be unaware they have been compromised, in coordination with other federal entities as appropriate.</li> </ul>
SRMAs	<ul style="list-style-type: none"> <li>▪ Assist in threat response by identifying and notifying similarly postured entities within a sector of emerging or known threats.</li> <li>▪ Support threat response with technical capabilities, as appropriate and requested.</li> <li>▪ Provide additional context based on sector-specific expertise and insight.</li> </ul>
Private Sector	<ul style="list-style-type: none"> <li>▪ May report and share information regarding cyber incidents and malicious cyber activity to appropriate federal entities.</li> </ul>

## Intelligence Support

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

374 **Federal LOE Lead Agency:** The Office of the Director of National Intelligence, through the Cyber  
 375 Threat Intelligence Integration Center, will lead coordinated intelligence support in response to a  
 376 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)	<ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ Provides threat reporting at levels of classification appropriate to the circumstances and demands of the incident, to include seeking declassification and/or downgraded reports.</li> <li>▪ Coordinates any intelligence collection, analysis, and production activities that may take place as part of the incident through the National Intelligence Manager for Cyber.</li> </ul>
CISA  SRMAs	<ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ Coordinates the sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents across the federal government.</li> <li>▪ Facilitating, in coordination with CISA, access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure,</li> <li>▪ 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.</li> <li>▪ 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.</li> </ul>
DOJ/FBI	<ul style="list-style-type: none"> <li>▪ Provides sharable intelligence gathered through threat response activities.</li> </ul>
All IC Components	<ul style="list-style-type: none"> <li>▪ Provides intelligence support as requested under ODNI coordination.</li> </ul>

### 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



380 adverse financial impacts; protection of privacy; managing liability risks; complying with legal and  
381 regulatory requirements (including disclosure and notification); engaging in communications with  
382 employees or other affected individuals; and dealing with external affairs.

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

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

390 Summary of Federal Civilian Executive Branch Entity Roles and Responsibilities:

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

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

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

---

<sup>20</sup> FCEB operational procedures are covered in detail in the [Federal Government Cybersecurity Incident and Vulnerability Response Playbooks](#).

## Annex E: Follow-On Implementation Activities

408 This NCIRP provides a foundational framework for national coordination of cyber incident response.  
 409 Further work is needed to fully implement this framework in operations across the national  
 410 stakeholder community. **Table 10** lists follow-on activities that can help more fully realize  
 411 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

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

- 413     ▪ **National Institute of Standards and Technology**
- 414         ○ [Incident Response, Overview](#)
- 415         ○ [Incident Response, Preparation Resources](#)
- 416         ○ [Incident Response, Life Cycle Resources](#)
- 417     ▪ **Cybersecurity and Infrastructure Security Agency**
- 418         ○ [Incident Response Plan \(IRP\) Basics \(cisa.gov\)](#)
- 419         ○ [Free Cybersecurity Services & Tools | CISA](#)
- 420     ▪ **Information Sharing and Analysis Centers**
- 421         ○ [National Council of ISACs - Member ISACs](#)
- 422     ▪ **Information Sharing and Analysis Organization Standards Organization**
- 423         ○ [Information Sharing Groups Browser – ISAO Standards Organization](#)
- 424     ▪ **Cybersecurity resources for U.S. State, Local, Tribal, and Territorial (SLTT) government**
- 425         **organizations**
- 426         ○ [CISA resources for SLTT Governments](#)
- 427         ○ [Multi-State ISAC](#)
- 428         ○ [Elections Infrastructure ISAC](#)
- 429         ○ [Tribal ISAC](#)
- 430     ▪ **Sector Specific Resources**
- 431         ○ Chemical Sector: [Chemical Sector Cybersecurity Resources](#)
- 432         ○ Commercial Facilities Sector: [Commercial Facilities Sector Cybersecurity Framework](#)
- 433             [Implementation Guidance | CISA](#) – [Media+Entertainment ISAC](#) – [Real Estate ISAC](#) –
- 434             [Retail and Hospitality ISAC](#)
- 435         ○ Communications Sector: [Communications and Cyber Resiliency Toolkit | CISA](#) and
- 436             [Network Reliability Resources | Federal Communications Commission \(fcc.gov\)](#) –
- 437             [Communications ISAC](#) – [Small Broadband Provider ISAC](#)
- 438         ○ Critical Manufacturing Sector: [Critical Cybersecurity Manufacturing Sector Resources](#)
- 439         ○ Dams Sector: [Dams Sector Cybersecurity Capability Maturity Model \(C2M2\) 2022 | CISA](#)
- 440         ○ Defense Industrial Base Sector: [Defense Industrial Base \(DIB\) Cybersecurity Portal](#)
- 441             [\(dod.mil\)](#) – [National Defense ISAC](#)
- 442         ○ Emergency Services Sector: [Emergency Services Cybersecurity Initiative](#) – [Emergency](#)
- 443             [Management and Response ISAC](#)
- 444         ○ Energy Sector: [Cybersecurity | Department of Energy](#) – [Downstream Natural Gas ISAC](#) –
- 445             [Electricity ISAC](#) – [Oil and Natural Gas ISAC](#)
- 446         ○ Financial Services Sector: [Financial Institutions | U.S. Department of the Treasury](#) – [FDIC](#)
- 447             [Cybersecurity Resources](#) – [Financial Services ISAC](#)

- 448 ○ Food and Agriculture Sector: [Food and Ag ISAC](#)
- 449 ○ Government Services and Facilities Sector: [Research and Education Networks ISAC](#)
- 450 ○ Health and Public Health Sector: [HC3 Products | HHS.gov](#) - [Health ISAC](#)
- 451 ○ Information Technology Sector: [IT-ISAC](#)
- 452 ○ Nuclear Reactors, Materials, and Waste Sector: [Nuclear Sector Cybersecurity](#)
- 453 [Framework Implementation Guidance | CISA](#) and [US Nuclear Regulatory Commission](#)
- 454 [Cybersecurity Resources](#)
- 455 ○ Transportation Systems Sector: [Department of Transportation Cybersecurity Resources](#)
- 456 and [Cybersecurity Resources for Transit Agencies | FTA \(dot.gov\)](#) - [Automotive ISAC](#) -
- 457 [Aviation ISAC](#) - [Maritime ISAC](#) - [Maritime Transportation System ISAC](#) - [Surface](#)
- 458 [Transportation, Public Transportation, and Over-the-Road Bus ISACs](#)
- 459 ○ Water and Wastewater Systems Sector: [EPA Cybersecurity for the Water Sector | US EPA](#)
- 460 - [Water ISAC](#)
- 461 ■ **Multi Sector Resources**
- 462 ○ [Space ISAC](#)

## Annex G: Authorities and Statutes

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

466     **■ Homeland Security, Resilience, and Emergency Response**

- 467         ○ Cybersecurity and Infrastructure Security Agency Act of 2018
- 468         ○ Homeland Security Act of 2002, as amended
- 469         ○ Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended
- 470         ○ EO 13618: Assignment of National Security and Emergency Preparedness  
471             Communications Functions
- 472         ○ PPD-8: National Preparedness
- 473         ○ NSM-22: Critical Infrastructure Security and Resilience
- 474         ○ PPD-40: National Continuity Policy
- 475         ○ PPD-41: U.S. Cyber Incident Coordination Policy, and its accompanying Annex
- 476         ○ HSPD-5: Management of Domestic Incidents

477     **■ Information and Communication Technology**

- 478         ○ Title 47-Telecommunications
- 479         ○ Cyber Incident Reporting for Critical Infrastructure Act of 2022
- 480         ○ Communications Act of 1934, Section 706
- 481         ○ Cybersecurity Act of 2015
- 482         ○ National Cybersecurity Protection Act of 2014
- 483         ○ EO 13636: Improving Critical Infrastructure Cybersecurity
- 484         ○ EO 13691: Promoting Private Sector Cybersecurity Information Sharing
- 485         ○ EO 13800: Strengthening the Cybersecurity of Federal Networks and Critical  
486             Infrastructure
- 487         ○ EO 14028: Improving the Nation's Cybersecurity
- 488         ○ National Security Memorandum (NSM) 5: Improving Cybersecurity for Critical  
489             Infrastructure Control Systems
- 490         ○ National Cybersecurity Strategy of 2023

491     **■ Federal Information and Communication Technology Systems**

- 492         ○ Federal Information Security Modernization Act of 2014
- 493         ○ National Security Directive 42: National Policy for the Security of National Security  
494             Telecommunications and Information Systems
- 495         ○ NSPD-54/HSPD-23: Cybersecurity Policy
- 496         ○ NSM 8: Improving the Cybersecurity of National Security, Department of Defense (DoD),  
497             and Intelligence Community Systems

- 498 ○ OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally
- 499 Identifiable Information.
- 500 ○ OMB M-21-31 Improving the Federal Government's Investigative and Remediation
- 501 Capabilities Related to Cybersecurity Incidents
- 502 ■ **Federal Statutory Mechanisms for Prosecuting Cybercrime**
- 503 ○ Computer Fraud and Abuse Act (CFAA)
- 504 ○ Stored Communications Act
- 505 ○ Economic Espionage Act of 1996, as amended by the Defend Trade Secrets Act of 2016
- 506 ○ Wire Fraud statute
- 507 ■ **National Security, Intelligence, and Law Enforcement**
- 508 ○ Title 6 – Domestic Security
- 509 ○ Title 10 – Armed Forces
- 510 ○ Title 18 – Crimes and Criminal Procedure
- 511 ○ Title 32 – National Guard
- 512 ○ Title 50 – War and National Defense
- 513 ○ Intelligence Reform and Terrorism Prevention Act of 2004
- 514 ○ National Security Act of 1947, as amended
- 515 ○ EO 12333: United States Intelligence Activities, as amended
- 516 ○ EO 12829: National Industrial Security Program, as amended
- 517 ○ EO 12968: Access to Classified Information, as amended
- 518 ○ EO 13549: Classified National Security Information Programs for State, Local, Tribal,
- 519 and Private Sector Entities
- 520 ○ EO 12829: National Industrial Security Program, as amended
- 521 ○ Secretary of Defense Memorandum, "Delegation of Authority to Make Arrangements
- 522 with Private Sector Entities Pursuant to Section 1642(b) of the National Defense
- 523 Authorization Act for Fiscal Year 2019," dated 1 October 2022
- 524 ■ **Additional authorities in times of a national emergency declared by the President or**
- 525 **Congress, a declaration of war, and other situations in which a state of war may exist absent**
- 526 **a declaration of war:**
- 527 ○ 10 USC §12301 et seq. governing the activation of reserve forces
- 528 ○ Defense Production Act of 1950, as amended
- 529 ○ 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
------------	-----------------------------