National Cyber Incident Response Plan

Interim Version, September 2010

Homeland Security

[This page intentionally left blank]

PREFACE

[This page intentionally left blank.]

[Undergoing internal DHS preface coordination.]

For more information please contact NCCIC@dhs.gov

[This page intentionally left blank.]

TABLE OF CONTENTS

FOREWORD

The rapidly converging information technology (IT) and communications infrastructure, known as "cyberspace"[1], touches every corner of the globe and every facet of human life. The United States in particular continues to embrace the cyber domain, utilizing it for diverse activities from increasing energy efficiency to conducting financial transactions. Recognizing this national reliance on cyberspace and the interdependent nature of the Nation's current cyber infrastructure, the President commissioned the Cyberspace Policy Review. This report, released on May 29, 2009, builds on the Comprehensive National Cybersecurity Initiative (CNCI) and calls for the development of a "cybersecurity incident response plan."

This National Cyber Incident Response Plan (NCIRP) was developed according to the principles outlined in the National Response Framework (NRF) and describes how the Nation responds to Significant Cyber Incidents. While the NRF provides the Nation with "guiding principles that enable all response partners to prepare for and provide a unified national response," the NRF Incident Annexes provide guidance on how to address specific contingency or hazard situations.

The Cyber Incident Annex to the NRF (Appendix A) was developed in tandem with the NCIRP. It describes the appropriate organizations for the Secretary of Homeland Security to rely on and briefly outlines the contents of the NCIRP, including the policies, organizations, actions, and responsibilities for a nationally coordinated, broad-based approach to cyber incidents. The NCIRP expands on the NRF Cyber Incident Annex to address the unique operational response structure and lifecycle required for Significant Cyber Incidents.

The NCIRP is built on the foundations of the NRF and is intended to facilitate coordination with NRF mechanisms during cyber incidents with physical consequences. Therefore, cyber incident responders are strongly encouraged to familiarize themselves with the NRF, the Cyber Incident Annex, and the National Incident Management System (NIMS), as well as the NCIRP. Supporting sector and organizational operational plans will provide specific details on preparedness, response, and recovery activities in alignment with the NCIRP and in concert with the NRF, NIMS, and National Infrastructure Protection Plan (NIPP).

[1] Cyberspace: A global domain of operations consisting of the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.

[This page intentionally left blank.]

1 INTRODUCTION

Cyberspace is a modern technological domain that helps drive progress in everything from scientific innovation to international trade. Yet the foundations of the cyber domain remain vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in cyberspace can be exploited for nefarious purposes by both nation-states and non-state actors.

The risks associated with the Nation's dependence on cyberspace led to the development of the Comprehensive National Cybersecurity Initiative and the Cyberspace Policy Review. These initiatives enhanced the national cybersecurity posture by creating a more robust front line of defense, enhancing shared situational awareness, augmenting offensive capabilities in support of network defense, and moving toward "network speed" responses, among other activities.

The NCIRP is designed in full alignment with these initiatives to ensure that Federal cyber incident response policies facilitate the rapid national coordination needed to defend against the full spectrum of threats. The NCIRP focuses on improving the human and organizational responses to cyber incidents, while parallel efforts focus on enhancing the community's technological capabilities.

In the current risk environment, cyber incidents occur every day, often cascading across Federal, State, Local, Tribal, Territorial, and private sector systems. Cyberspace's cross-jurisdictional and interdependent nature requires effective partnerships across these traditional boundaries. The Federal Government and the Nation are highly dependent on IT and communications infrastructure provided by the private sector, and this dependency underscores the need for flexibility and partnership across a wide variety of communities. As the owners and operators of these vital assets, the private sector's expertise and experience with emergency and incident management must be integrated into any truly national cyber incident response plan.

With these interdependencies in mind, the NCIRP was developed in close coordination with Federal, State, Local, Territorial and private sector partners. It provides a strategy for rapidly coordinating the operational response activities of Federal, State, Local, Tribal, and Territorial governments; the private sector; and international partners during cyber incidents.

1.1 PURPOSE

The purpose of the NCIRP is to establish the strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident. It ties various policies and doctrine together into a single tailored, strategic, cyber-specific plan designed to assist with operational execution, planning, and preparedness activities and to guide short-term recovery efforts.

1.2 SCOPE

The NCIRP is a strategic plan for operational coordination and execution among Federal, State, Local, Tribal, and Territorial governments; the private sector; and international partners. More detailed operational plans will support the NCIRP at the sector and organizational levels. In all

cases, incident response activities will be conducted in accordance with applicable law and policy.[2]

The NCIRP sets the strategic direction for how the Nation responds to everyday cyber incidents and how these steady-state operations are escalated into nationally coordinated response activities. Although steady-state activities and the development of a common operational picture are key components of the NCIRP, the plan focuses primarily on building the mechanisms needed to respond to a Significant Cyber Incident.

Significant Cyber Incident A Significant Cyber Incident is a set of conditions in the cyber domain that requires increased national coordination.[3] This increase in national coordination is triggered when the National Cyber Risk Alert Level (NCRAL) system reaches Level 2 (Appendix K).

The NCRAL system[4] takes into account the threats, vulnerabilities, and potential consequences across the cyber infrastructure and will provide an indication of the overall national cyber risk. This system will also take into account the conditions outlined in Homeland Security Presidential Directive 5 (HSPD-5) when applied to the cyber domain[5] and will focus primarily on cyber incidents that impact:

- National security
- Public health and public safety
- National economy, including any of the individual sectors that may affect the national economy
- Public confidence
- Any combination of these categories at the national, regional, or sector level[6]

2 Nothing in this plan restricts, supersedes, or otherwise replaces the legal authorities or regulatory responsibilities of any government agency or organization. All information will be handled, transmitted, distributed, released, and/or stored in accordance with the standards, caveats, and procedures described by the originating agency, regulatory governance, and/or law. For more information on legal authorities, please see Appendix L.

3 Coordination assistance may be requested for incidents that do not reach Level 2 and without triggering full national coordination activities, such as the Cyber Unified Coordination Group (UCG). However, such activities must also inform the common operational picture to help determine the National Cyber Risk Alert Level (NCRAL) system.

4 The NCRAL takes into account a variety of public and private sector alert level systems. However, the Department of Homeland Security and Department of Defense (DOD) are in the process of leading an interagency effort to develop a national alert level system that more fully integrates the NCRAL with a variety of DOD alert levels.

5 These conditions include when the confidentiality, integrity or availability of systems is affected and (1) a Federal department or agency acting under its own authority has requested the assistance of the Secretary; (2) the resources of State and Local authorities are overwhelmed and Federal assistance has been requested by the appropriate State and Local authorities; (3) more than one Federal department or agency has become substantially involved in responding to the incident; or (4) the Secretary has been directed to assume responsibility for managing the domestic incident by the President.

6 Coordination and assistance may be requested at any level without requiring the activation of full national coordination structures, such as the Cyber UCG Incident Management Team (IMT). Furthermore, structures like the Cyber UCG IMT may be activated in order to prevent incidents from occurring in accordance with the standard operating procedures of the National Cybersecurity and Communications Integration Center and its partner agencies.

Level	Label	Description of Risk	Level of Response
1	**Severe**	Highly disruptive levels of consequences are occurring or imminent	Response functions are overwhelmed, and top-level national executive authorities and engagements are essential. Exercise of mutual aid agreements and Federal/non-Federal assistance is essential.
2	**Substantial**	Observed or imminent degradation of critical functions with a moderate to significant level of consequences, possibly coupled with indicators of higher levels of consequences impending	Surged posture becomes indefinitely necessary, rather than only temporarily. The Department of Homeland Security (DHS) Secretary is engaged, and appropriate designation of authorities and activation of Federal capabilities such as the Cyber UCG take place. Other similar non-Federal incident response mechanisms are engaged.
3	**Elevated**	Early indications of, or the potential for but no indicators of, moderate to severe levels of consequences	Upward shift in precautionary measures occurs. Responding entities are capable of managing incidents/events within the parameters of normal, or slightly enhanced, operational posture.
4	**Guarded**	Baseline of risk acceptance	Baseline operations, regular information sharing, exercise of processes and procedures, reporting, and mitigation strategy continue without undue disruption or resource allocation.

Table 1: National Cyber Risk Alert Levels

During a Significant Cyber Incident, DHS, through its National Cybersecurity and Communications Integration Center (NCCIC), coordinates national response efforts and works directly with Federal, State, Local, Tribal, and Territorial governments and private sector partners.

2 NATIONAL CONCEPT OF OPERATIONS

Cyberspace is a cross-sector, multijurisdictional operational domain that is heavily dependent on private sector owners and operators. Effective response requires close coordination across traditional boundaries and requires the development of a robust common operational picture as a foundational element.

2.1 COMMON OPERATIONAL PICTURE

Effectively understanding risks in cyberspace requires that a wide range of departments, agencies, and organizations collaborate on a daily basis to identify threats, vulnerabilities, and potential consequences. The NCIRP integrates and builds on current efforts to connect Federal cybersecurity centers and moves the Nation toward a more robust common operational picture capable of bringing together Federal, State, Local, Tribal, and Territorial resources; critical infrastructure and key resources (CIKR); and private sector perspectives.[7]

DHS integrates and maintains this national common operational picture for cyberspace via the NCCIC with the direct assistance and participation of the organizations described below and in Section 2.3.[8] The NCCIC provides cross-domain situational awareness,[9] including "a

[7] The NCCIC integrates the functions of the National Cyber Security Center (NCSC), U.S. Computer Emergency Readiness Team (US-CERT), National Coordinating Center (NCC), and Industrial Control Systems CERT (ICS-CERT) into a single coordination and integration center and co-locates other essential public and private sector cybersecurity partners as described in Sections 3.1 and 3.2.

[8] The NCCIC is an operational element of the Office of Cybersecurity and Communications (CS&C) in the DHS National Protection and Programs Directorate (NPPD). All references to CS&C and NPPD include any successor organization within DHS with the authorities and missions for the security of cyberspace.

continuously updated, comprehensive picture of cyber threats," vulnerabilities, and consequences to provide "indications and warning of imminent incidents, and to support a coordinated incident response."[10] Situational awareness from this effort will be provided to appropriate parties at the appropriate level of detail and classification. Situational awareness will be provided to the National Infrastructure Coordinating Center (NICC) and the National Operations Center (NOC) to enhance the national common operating picture for the President; Secretary; Federal, State, Local, Tribal, and Territorial homeland security partners; private sector; and nongovernmental organizations (NGO).

Information for the common operational picture will come from a variety of sources, including—

- Federal departments and agencies
- The national security community and Intelligence Community (IC)
- The law enforcement community, including Federal, State, and Local law enforcement agencies
- Various public and private sector sources, such as Information Sharing and Analysis Centers (ISACs) and private sector companies
- Cybersecurity vendors
- Open sources, such as presentations from cyber risk-related conferences.

Although this common operational picture is a foundation for cyber incident response activities, effective response operations in the cyber domain require the coordination and execution of a wide variety of legal and operational authorities. These activities will be centrally coordinated but executed in a decentralized fashion based on organizational responsibilities.

2.2 CENTRALIZED COORDINATION, DECENTRALIZED EXECUTION

The United States depends on a decentralized IT and communications infrastructure. Over the last several decades, the United States has developed legal authorities that are similarly decentralized. Each incident response partner has capabilities, authorities, and legally mandated roles to play in securing cyberspace. These authorities have traditionally been executed independently, but as noted in the Cyberspace Policy Review and confirmed by experience, "the status quo is no longer acceptable." The threats and risks to the Nation's information and communications technology infrastructure require the Nation to move beyond legacy organizational stovepipes.

As with the NRF, the NCIRP leverages existing authorities and relationships to coordinate the execution of incident response activities according to each organization's roles and responsibilities.

2.3 GENERAL ROLES AND RESPONSIBILITIES FOR CYBER INCIDENTS

A cyber incident may rapidly spread across interdependent and cross-jurisdictional networks, and Significant Cyber Incidents may quickly require nationally coordinated response actions based on differing authorities and priorities. The NCCIC will provide the facility and mechanisms to coordinate national response efforts. The following organizations will play key roles in this

---

9 Cross-Domain Situational Awareness: The set of timely cross-domain national-level information that will provide situational awareness on the state of U.S. cyber networks and systems to (1) know the availability, integrity, and confidentiality of U.S. cyber networks and systems; (2) understand the current and potential threats to U.S. cyber networks and systems; and (3) ensure that legitimate network operations are not mistaken for malicious activity.

10 Cyberspace Policy Review, p. 24. Available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

coordinated effort and will bring their authorities and capabilities to bear during a Significant Cyber Incident. More detailed responsibilities for each organization can be found in Appendices B through J.

Executive Office of the President (EOP): The President of the United States leads the Federal Government's response effort to ensure the necessary coordinating structures, leadership, and resources are applied quickly and efficiently to large-scale and catastrophic incidents. The EOP has a variety of structures in place to provide the President with national strategic and policy advice.

Department of Homeland Security: The Secretary of Homeland Security is the principal Federal official for domestic incident management. Through CS&C, the Secretary of Homeland Security is responsible for providing crisis management and coordination in response to Significant Cyber Incidents; coordinating and integrating information from the Federal cybersecurity centers; State, Local, Tribal, and Territorial governments; and the private sector; and generally maintaining an organization to serve as a focal point for the security of cyberspace.[11] These responsibilities are executed through the NCCIC in coordination with a variety of partner organizations. DHS will be responsible for providing consolidated reports to the EOP.

Although the NCCIC's coordination role does not change existing department and agency authorities or missions, DHS, through the NCCIC, coordinates with all partners, including law enforcement agencies, in the national effort to investigate and prosecute cybercrime; the IC regarding threats and IC activities, intelligence, and attribution; Department of Defense (DOD) elements regarding intelligence and information sharing, and military operations to defend the homeland; State, Local, Tribal, and Territorial governments; and the private sector to ensure all response organizations are leveraging a common operational picture as they execute their individual authorities and missions.

It is anticipated that a wide range of activities may be needed in response to any cyber incident, some of which focus on activities that are clearly within the authorities of a single department or agency. For example, the Federal Bureau of Investigation (FBI) or U.S. Secret Service (USSS) may engage in extensive investigative activities in connection with a major incident, but only a subset of those activities—those associated with preventing, stopping, or remediating network or related impacts on CIKR infrastructures—need to be formally coordinated with the NCCIC. However, the DHS NCCIC must maintain situational awareness throughout steady-state and Significant Cyber Incident response activities. Therefore, all Federal organizations must provide information on their ongoing cyber-related operations to the extent permitted by law to inform the common operational picture and assist coordination and deconfliction efforts, as needed. Cyber Unified Coordination Group (UCG) Incident Management Team (IMT) members (described in Section 3.2) will keep each other informed of the full range of activities engaged in by their respective organizations in connection with a given incident for situational awareness purposes.

Department of Defense: DOD maintains and employs Armed Forces to support and defend the Constitution of the United States against all enemies, foreign and domestic; ensure, by timely and effective military action, the security of the United States, its possessions, and areas vital to

[11] In accordance with HSPD-5, HSPD-7, HSPD-23/National Security Presidential Directive 54 (NSPD-54), and National Infrastructure Protection Plan (NIPP).

its interest; and uphold and advance the national policies and interests of the United States. Among other missions, DOD establishes and maintains shared situational awareness and directs the operation and defense of the .mil network.

DOD entities responsible for computer security and computer network defense of DOD systems may exercise those duties in support of the national response effort in four primary roles: (1) Defense Support of Civil Authorities; (2) intelligence and information sharing, (3) law enforcement investigations, and (4) military operations to defend the homeland.

National Security Agency: The National Security Agency/Central Security Service (NSA/CSS) is the lead for U.S. cryptologic work in Signals Intelligence (SIGINT)/ Computer Network Exploitation (CNE), Information Assurance (IA), and Network Threat Operations. NSA's support to DHS in the event of a cyber incident is provided as a DOD activity, in coordination with the Director of National Intelligence. Foreign intelligence support and IA support in connection with non-national security systems is provided to DHS per Executive Order 12333, as amended. In addition, the Director NSA is the designated National Manager for the security of National Security Systems in accordance with National Security Directive 42. Under these authorities, NSA conducts SIGINT/CNE activities for both national and DOD requirements and provides IA and Network Threat Operations support to National Security Systems, as well as to DHS for non-national security systems.

The NSA/CSS Threat Operations Center (NTOC) is the primary NSA/CSS partner for DHS response to cyber incidents. The NTOC establishes real-time network awareness and threat characterization capabilities to forecast, alert, and attribute malicious activity and enable coordination of Computer Network Operations by NSA/CSS; U.S. Strategic Command (USSTRATCOM); and the broader community of the United States, its allies, and its mission partners.

Department of Justice: The Attorney General (AG) is the principal law enforcement officer of the United States. The Department of Justice's (DOJ) mission is to enforce the law, defend the interests of the United States according to the law, and ensure public safety against threats, both foreign and domestic. The National Security Division of DOJ oversees all national security, foreign intelligence, and counterintelligence investigations, working with the appropriate U.S. Attorney's office(s). The Criminal Division of DOJ oversees criminal prosecutions, together with appropriate U.S. Attorney's offices. A cyber incident may involve many different components of DOJ, including the Criminal Division, the National Security Division, the Office of Legal Counsel, and the U.S. Attorney's offices. The Attorney General provides guidance on legal issues that require resolution during efforts to respond to, and recover from, a cyber incident; manages any resulting criminal and/or domestic foreign intelligence investigations; and shares information from those investigations as permitted by law.

Federal Bureau of Investigation: The FBI has a dual responsibility to prevent harm to national security as a member of the IC and to enforce Federal laws as part of DOJ. The FBI reports to both the Attorney General and the Director of National Intelligence. As a national security organization, the FBI serves as the lead agency operating domestically to protect and defend the United States against terrorist and foreign intelligence threats, including those that have a cyber nexus. As a law enforcement agency, the FBI is authorized to uphold and enforce the criminal laws of the United States not assigned exclusively to another Federal agency and has primary or concurrent jurisdiction over all Federal cybercrime laws. The FBI fulfills its intelligence and

criminal law enforcement roles through investigations, intelligence analysis, information dissemination, partner collaboration, and community outreach. The FBI leads the National Cyber Joint Investigative Task Force (NCIJTF) as the multiagency national focal point for coordinating cyber investigations across all national security and criminal law enforcement programs.

Department of State: The Department of State (DOS) formulates, coordinates, and provides oversight of foreign policy. During domestic crises, DOS is the primary point of contact for foreign governments abroad and liaises with foreign embassies and consulates in the United States regarding access to and protection of foreign nationals. In the event of a cyber incident, DOS serves as the principal point of contact for the foreign affairs community.

Sector Specific Agencies (SSA): In accordance with their responsibilities under the NIPP, SSAs will facilitate real-time cyber incident notification within their respective sectors and provide mechanisms for reporting this information to the NCCIC. SSAs manage the overall process for building partnerships and leveraging CIKR security expertise, relationships, and resources within their sector and are responsible for coordinating sector-level participation in the NCIRP, including supporting sector efforts to align cyber preparedness and response efforts with the NCIRP. SSAs and sector-designated operational entities may also communicate sector priorities and protective actions in the event of widespread impact to a sector. In addition to relationships within their sector, representatives of all sectors may coordinate directly with the NCCIC.[12]

Other Federal Departments and Agencies: Federal departments and agencies are responsible for maintaining a 24x7 security capability that is available and cleared to send, receive, and act on alerts at all levels of classification. They are responsible for ensuring all relevant department and agency cyber information is promptly transmitted to DHS to maintain common situational awareness. All agencies provide cyber-related expertise in support of the NCIRP and cyber incident response activities as further described in Section 3.1.

State, Local, Tribal, and Territorial Governments: Each Chief Executive of a State, Local, Tribal, or Territorial government is responsible for its cybersecurity preparedness, response, and recovery procedures as outlined in Appendix H. These responsibilities include identifying primary and secondary cyber incident response points of contact for each Chief Executive's respective government.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a key resource for State, Local, Tribal, and Territorial government information sharing, early warnings and alerts, mitigation strategies, training, and exercises and for maintenance of overall cyber situational awareness.

Private Sector: The private sector is made up of two primary groups: (1) private sector CIKR owners and operators and (2) the general private sector ("private sector"). Representatives from both groups are encouraged to coordinate and communicate directly with the NCCIC.[13]

CIKR owners and operators will be integrated both physically and virtually into the NCCIC during steady-state operations and will be fully and appropriately integrated into cyber incident

[12] Reporting to the NCCIC is not a substitute for any reporting required by law, regulation, or prior agreement.

[13] Coordination with the NCCIC occurs primarily through current methods, such as through NCC, US-CERT, ICS-CERT or other NCCIC partner. Reporting to the NCCIC is not a substitute for any reporting required by law, regulation, or prior agreement.

response capabilities.[14] As key owners, operators, and leaders in cyberspace and as a key part of NCCIC operations, CIKR owners and operators are likely to be called upon to assist the Federal Government during a Significant Cyber Incident.

Multiple ISACs will likely play a key role during steady state and will be crucial during a cyber incident. By definition, ISACs are CIKR sector-specific, trusted communities of security specialists that identify, analyze, and share information; collaborate on threats, incidents, vulnerabilities, and best practices; and generally work to protect their respective industries from cyber and physical threats. CIKR sector organizations are encouraged to coordinate with ISACs when possible to assist in information sharing, analytics, and trend definition. Sectors and industries without ISACs should engage with their SSA, Sector Coordinating Council (SCC), or sector-designated operational entities to share information in a manner that is most effective for their sector.

In addition, many private sector companies have established organizational watch and warning centers. These functions may manifest themselves as security operations centers, network operations centers, or computer emergency response teams (CERT), but they all promote connectivity and security of their respective networks. Elements inside the NCCIC work with operators of these entities during steady state to maintain accurate, up-to-date information on cybersecurity threats and vulnerabilities in order to facilitate communications during a cyber incident.

Non-Governmental Organizations: Non-governmental organizations (NGOs) can provide assistance as needed and requested. They can help develop and implement sustainable strategies for effectively mitigating and addressing the consequences of a cyber incident and can provide essential services and expertise. These may include ad-hoc groups that come together to address a specific problem or well-established groups that have operated for years. The NCCIC will work with its partners to identify NGOs to engage with and to develop engagement plans and coordination mechanisms for these relationships.

International Coordination: While DOS coordinates diplomatic outreach and formal international agreements, other Federal departments and agencies, including DHS, DOD, DOJ, the FBI, and USSS, have active multilateral and bilateral partnerships. These partnerships include efforts related to watch and warning, incident response, information sharing, CIKR interdependencies, cyber laws, and procedures. Further, many IT and communications sector businesses and providers are multinational businesses with critical international elements and relationships, including interaction with both policy and operational communities around the world.

Due to these cross-cutting and multifaceted networks of key associations, those best informed of the cultural, legal, and political nuances of that international entity must individually manage these relationships to maintain trust and international agreements. Those with formalized international relationships should work to build on and maintain these relationships during steady-state operations. The NCCIC will work in coordination with DOS, DOD, DOJ, DNI, and the FBI; private sector; and other partners to ensure agency activities are synchronized and deconflicted over time.

[14] Because of the large number of CIKR owners and operators, it is likely that only those affected by the current threat or vulnerability would physically integrate onto the NCCIC floor. However, there may be specific circumstances where others need to be brought in to help mitigate the consequences of any response actions.

Figure 1 depicts the general Federal incident management "lanes" as described above. State, Local, Tribal, and Territorial lanes will be defined by each entity's specific roles, responsibilities, and authorities.

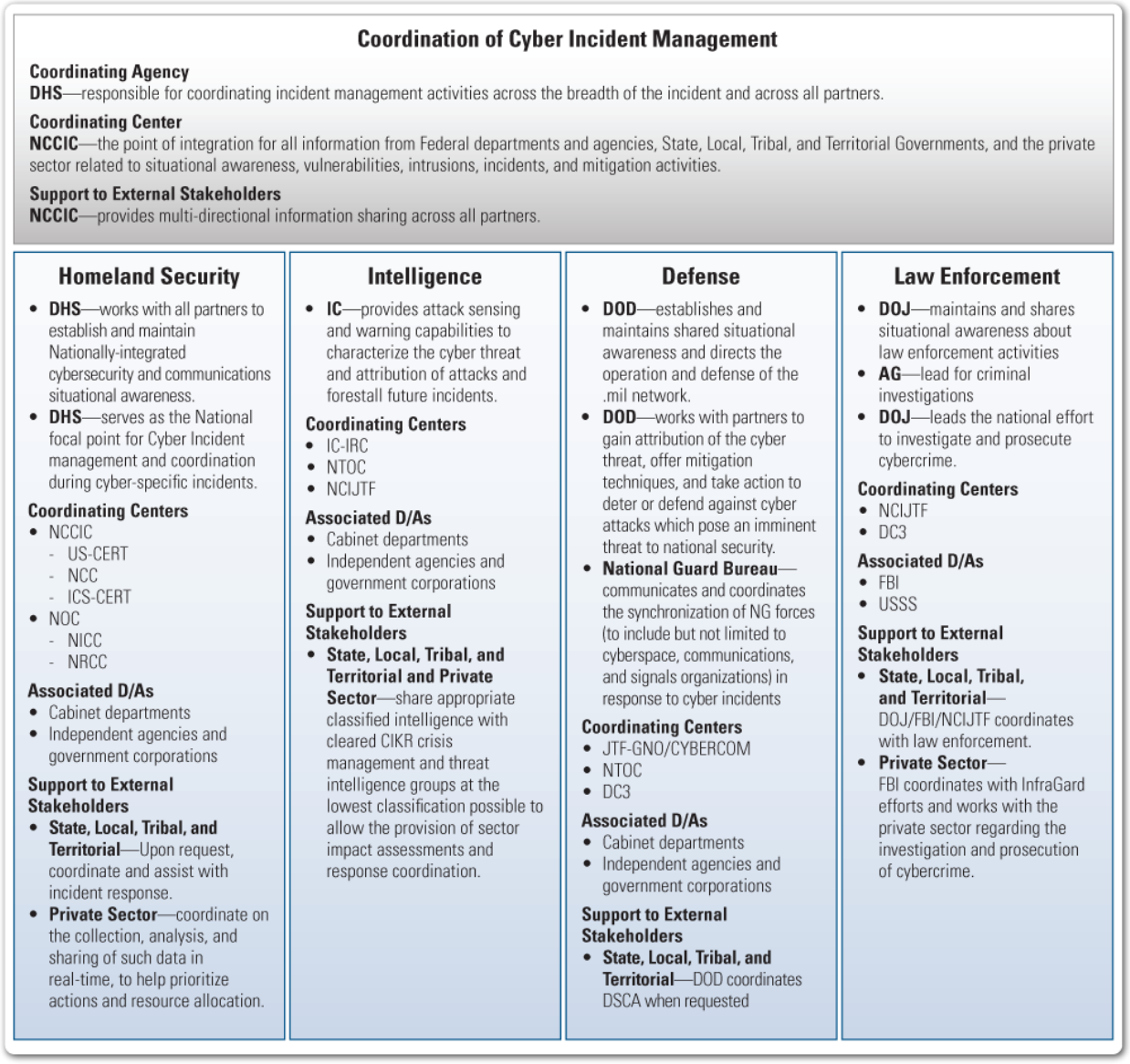


Figure 1: Federal Cyber Incident Lanes

Because of the diverse and potentially divergent priorities, interests, and needs of these response partners, the NCCIC works to harmonize response efforts during steady state and coordinates the development and, as appropriate, execution of response activities for Significant Cyber Incidents.

2.4 SUPPORTED AND SUPPORTING RELATIONSHIPS

Agencies and organizations with roles and responsibilities during a cyber incident have a variety of support relationships that require routine information sharing, deconfliction, collaboration, and, at times, joint action. The exact nature of each support relationship will depend on the nature, severity, and scope of each incident. There will be situations where DHS, through the

NCCIC and its partners, will be the primary supported organization for operational execution and coordination for an incident. In other situations, DHS, through the NCCIC and its partners, will support other response partners in executing their mission.

DHS as a Supported Organization

DHS is the primary organization for coordinating national activities during cyber incidents. It will receive support and assistance from other departments, agencies, components, and organizations and will coordinate operational activities related to cybersecurity and communications during Significant Cyber Incidents.

The NCCIC also receives support from other elements of DHS on issues related to cybersecurity, intelligence, infrastructure protection, and operations coordination to ensure the NCCIC and its partners fully recognize when cyber events may have cascading effects. This support allows NCCIC partners to work to prevent cascading effects, properly evaluate cyber risk across sectors, and communicate this risk through the NCRAL system. Within DHS, the NICC and the NOC provide further support to NCCIC operations by assisting with the dissemination of information and providing advice and assistance as needed.

DHS as a Supporting Organization

While many organizations work to support and enable NCCIC activities, in many circumstances, the NCCIC provides support to other organizations. During steady state, the NCCIC supports the missions of partner organizations by providing situational awareness related to cyber operations, cyber risk, and overall status of the IT and communications CIKR sectors. If damage occurs to IT or communications infrastructure during a natural disaster such as a hurricane, the NCCIC supports the Federal Emergency Management Administration (FEMA) and any Joint Field Office established at the incident site. The NCCIC, through the capabilities provided by the National Coordinating Center for Telecommunications (NCC), similarly supports the National Communications System (NCS) effort to restore communications in accordance with Emergency Support Function -2 (ESF #2).[15]

In extraordinary circumstances, the President, as Commander in Chief, or Congress may authorize military actions to counter threats to the United States. Therefore, DOD may conduct military missions as the lead in defending the United States. In such circumstances, DHS, via the NCCIC, works through its processes and with its partners to support overall DOD missions.

Simultaneous Supported and Supporting Relationships

The authorities and capabilities of each entity often must change in size, scope, and complexity as situations evolve.[16] In a number of potential scenarios, the NCCIC would be both a supported and supporting organization. A few examples are described below. In these cases, the NCCIC continues to receive national-level support for coordinating operational execution in the cyber domain while it supports other national-level efforts.

For example, in a number of circumstances, a cyber incident can have physical consequences by disrupting industrial control systems or by other means. These effects may or may not require national assistance or coordination.

---

[15] The NCCIC remains a supported organization for the purposes of coordinating operational execution in support of FEMA and the NOC.

[16] In Significant Cyber Incidents where joint action is required, supported and supporting relationships may change from phase to phase in an operation and will require formal processes to be established.

Minor, Localized Physical Effects: If a cyber event leads to minor, localized effects, it is handled at the local jurisdictional level. The NCCIC coordinates national cyber operations to respond to the cyber causes of the incident and assists in mitigating or responding to their effects. The local jurisdiction responds to the effects, and the NOC, NICC, and other partners monitor and prepare for any national-level consequences.

Complex Incidents: As incidents become more complex, incorporating cyber and physical effects, more agencies and organizations may need to become involved. For example, if an incident requires national coordination from a Joint Field Office, the NCCIC continues to receive support for conducting operations in the cyber domain while supporting the NOC, NICC, National Response Coordination Center (NRCC), and other partner informational and operational needs. If needed, joint response operations are conducted according to established procedures, with the NCCIC supporting these efforts. In such cases, the NCCIC continues to receive support from its partners to coordinate the operational execution in the cyber domain. Although many organizations work to support and enable NCCIC activities, in many circumstances, the NCCIC provides support to other organizations.

During a complex incident, the Secretary of Homeland Security may choose to activate the DHS Crisis Action Team (CAT). The Secretary may partially or fully implement the CAT depending on the severity, magnitude, or scope of an incident. In these cases, the Director of Operations and the Assistant Secretary for CS&C coordinate the efforts of the DHS CAT and the NCCIC UCG (described in Section 3.1) to provide integrated support and guidance to the Secretary on all aspects of the incident, including cyber aspects.

NCCIC Flexibility

The NCCIC uses an Incident Command System organizational model to ensure the core organizations needed to execute these supported and supporting relationships are fully integrated into NCCIC operations. A key element of NCCIC operations is flexibility in execution to allow the NCCIC and partner entities to adapt rapidly to changing circumstances. To coordinate and assist in response efforts regardless of size and scope, the NCCIC routinely collaborates with partner organizations on issues related to sharing information, coordinating and deconflicting actions, conducting analysis, assessment, and decision support activities, and developing common processes and joint plans. The detailed nature of these relationships will be reflected in operational playbooks and standard operating procedures (SOP).

3 ORGANIZATION OF THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

The NCCIC operates in two primary phases: steady-state response and Significant Cyber Incident response. The primary difference between the two is that steady-state activities are built so that nationally coordinated execution of authorities can be quickly and efficiently implemented. Building on steady-state operations also ensures that Significant Cyber Incident response activities are consistent with the processes, relationships, and agreements built over time.

3.1 NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER ORGANIZATION DURING STEADY STATE

Every day, the Federal, State, Local, Tribal, and Territorial governments and the private sector respond to threats to their networks, systems, and data. Responding to threats, vulnerabilities,

disruptions, and intrusions is the steady-state of cybersecurity operations. The NCCIC maintains a 24x7 common operational picture during steady-state to enhance all partners' cybersecurity efforts, inform the national cyber risk picture, and facilitate incident response activities.

Overview of the NCCIC

The NCCIC is a 24x7 integrated cybersecurity and communications operations center, and the focal point of coordination for national response efforts to Significant Cyber Incidents. The NCCIC is also the national point of execution for response activities within the scope of DHS authorities and for response partners that choose to execute their authorities from the NCCIC. The NCCIC serves as a centralized location where the operational elements involved in cyber response activities are coordinated and where many partners are physically and virtually co-located.[17] It is the national point of integration for all cyber information provided by Federal departments and agencies; State, Local, Tribal, and Territorial governments; and the private sector related to situational awareness, vulnerabilities, intrusions, incidents, and mitigation activities. The NCCIC works with its partners to integrate cyber incident information from across the Federal civilian department and agency domain (.gov); defense domain (.mil); IC networks; law enforcement sources; and State, Local, Tribal, and Territorial domains—from critical private sector networks that have volunteered information to be shared and from open-source information and coordination with the rest of the private sector. The NCCIC is capable of classified and unclassified operations and communications and uses the appropriate channels and portals to appropriately share that information.

The NCCIC is staffed and structured to be an "always on" multiagency incident response center with participation open to State, Local, Tribal, Territorial, and private sector partners. During steady-state operations, the NCCIC will utilize co-located partners and outreach mechanisms to coordinate steady-state cyber incident response activities and produce a common operational picture. Although each partner maintains its own operating mission, the execution of NCCIC's mission relies on coordinated operations, distributed execution, and common situational awareness.

The NCCIC and Partner Organizations

A number of DHS organizations operate full-time within the NCCIC or have a major presence in daily NCCIC operations. The U.S. Computer Emergency Readiness Team (US-CERT), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and NCC execute their missions under the daily supervision of the Director of the NCCIC, with elements of the DHS Office of Intelligence and Analysis (I&A) providing the NCCIC with vital additional capabilities and connections to the IC and with elements of the National Cyber Security Center (NCSC) providing connectivity to the other cybersecurity centers. Representatives from Federal departments and agencies, the IC, defense, law enforcement, other operations centers, and private sector organizations will be able to participate in the NCCIC physically and/or virtually according to agreements between the NCCIC and each organization.

[17] The NCCIC also includes substantial elements from the Communications Sector that will be responsible for additional activities, such as the restoration and operation of national security and emergency preparedness communications.

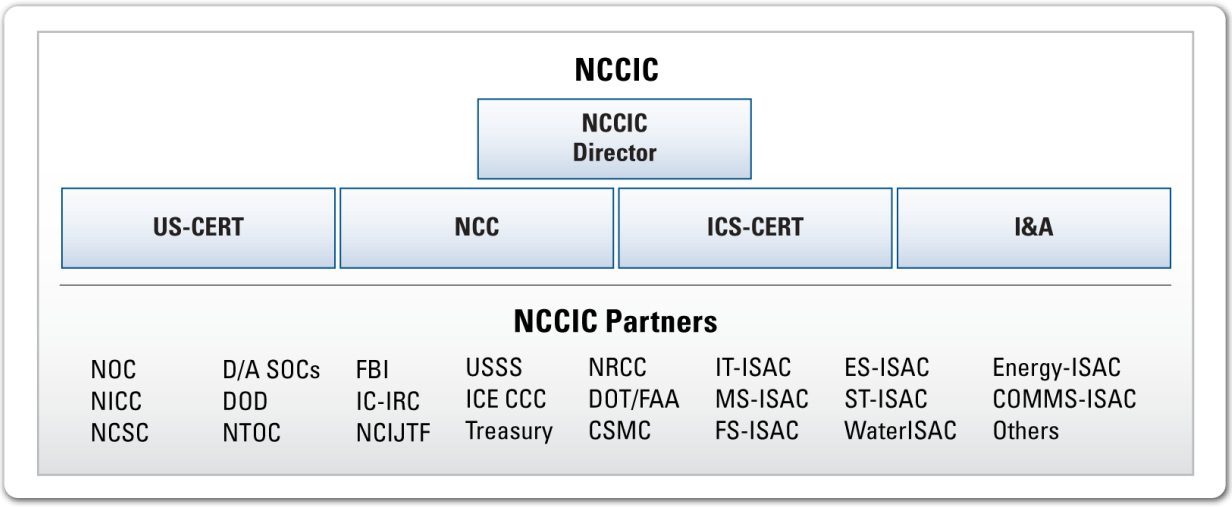


Figure 2: NCCIC and Partners

In addition to the partner entities listed in Figure 2, some of the critically important organizations that work in partnership with the NCCIC include—

- Other elements of DHS
  - United States Coast Guard
  - FEMA, NRCC, and FEMA Operations Center
- Other elements of DOD
- Other elements of NSA
- Other elements of the IC
- Other elements of DOJ
- DOS
- Department of the Treasury
- Department of Commerce (DOC), including the National Institute for Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA)
- Department of Energy (DOE)
- Department of Transportation/Federal Aviation Administration Cyber Security Management Center
- The 24 departments and agencies of the NCS
- Elements of other departments and agencies[18]
- EOP
- Additional ISACs and other sector-designated organizations upon request[19]
- Individual owners and operators of cybersecurity and communications CIKR, upon request and by agreement
- Owners and operators of Legislative Branch and Judicial Branch networks upon request.

In addition, many key private sector partners, States, Localities, Tribes, and Territories will play an integral role in NCCIC operations and a number of private sector partners will be

[18] All Federal departments and agencies have responsibilities for maintaining their IT and communications infrastructure.
[19] For the most up-to-date list of components and partners, please reference the NCCIC Concept of Operations (CONOPS).

indispensible to response operations because of the national dependence on the infrastructure they own and operate. Each of these NCCIC partners retains its own organizational and legal authorities and responsibilities. They work together with NCCIC leadership to build and maintain trusted relationships to enhance cybersecurity and communications collaboration, situational awareness, and everyday response capabilities.

Leadership

DHS Assistant Secretary of Cybersecurity and Communications

The Assistant Secretary for CS&C is responsible for leading DHS cybersecurity operations and coordinating these activities through the NCCIC. During steady state, the Assistant Secretary is responsible for working with the Cyber UCG to synchronize cybersecurity activities across Federal departments and agencies, State, Local, Tribal, and Territorial government, and private sector partners.

NCCIC Director

The NCCIC Director leads the daily activities of the NCCIC and reports to the DHS Assistant Secretary for CS&C. The Director is responsible for working with NCCIC partners to minimize and prevent disruptions to critical cyber infrastructure, respond to disruptions, and ensure the distribution of real-time incident information. The NCCIC Director, with the assistance of the Cyber UCG, is responsible for the development of national-level operational plans to synchronize the activities of operational partners. In addition, the Director will ensure awareness of partner capabilities and capacities to support incidents.

Cyber Unified Coordination Group[20]

The Cyber UCG is an interagency and inter-organizational coordination body that incorporates public and private sector officials.[21] It works during steady-state to ensure unity of NCCIC coordination and preparedness efforts and to facilitate the rapid response in case of a Significant Cyber Incident. The Cyber UCG is a pool of individuals that works to ensure centralized coordination and distributed execution take place. It is composed of senior officials and staff, that have been pre-selected by the leadership of their department, agency, or organization.[22]

As described below, each organization should designate at least two representatives: (1) a Cyber UCG Senior Official who has policy and decision-making authority and (2) a Cyber UCG Staff member who works for the Senior Official's organization but has been designated to participate in NCCIC preparedness efforts.[23] Cyber UCG Senior Officials and Staff meet and exercise regularly during steady state. Some organizations have multiple sets of authorities that may be needed during a Significant Cyber Incident. These organizations may pre-designate multiple Senior Officials provided a primary Senior Official is designated.[24]

During a Significant Cyber Incident, the Assistant Secretary coordinates with the appropriate Cyber UCG Senior Officials and Staff to activate the Cyber UCG IMT described in Section 3.1 and to develop and execute an incident action plan.

---

20 The UCG replaces the National Cyber Response Coordination Group (NCRCG).

21 The Cyber UCG is based on the principle of Unified Command outlined in the NIMS Incident Command System. The term UCG, along with other NIMS Incident Command System terms such as "Incident Management Team" and "incident action plan," are used to convey that the NCCIC intends to operate in accordance with these NIMS and Incident Command System principles.

22 Non-preselected UCG Senior Officials may need to be added to the UCG IMT based on the nature of a given cyber incident.

23 Each organization may choose whether its UCG Staff Member works with the NCCIC in a part-time or full-time capacity.

24 For example, DOD may choose to designate a Senior Official from the U.S. Cyber Command (USCYBERCOM) and a Senior Official from the U.S. Northern Command (USNORTHCOM) to exercise different sets of authorities.

Cyber Unified Coordination Group Senior Officials

Cyber UCG Senior Officials make up a pool of pre-designated, pre-trained, and situation-aware individuals who may be called on to represent their organization during a Significant Cyber Incident.[25] Each Federal department and agency head will designate at least one Cyber UCG Senior Official.[26] Each Chief Executive of a State, Locality, Tribe, or Territory and designated private sector CIKR partners will be requested to designate a Cyber UCG Senior Official. It is essential that these designations are made based on the authority of that individual's position and organization to quickly commit resources and make decisions to affect cyber incident response. Each Cyber UCG member should be able to—

- Understand and communicate the full range of response capabilities that his or her organization brings to bear
- Make decisions on behalf of his or her organization
- Quickly commit his or her agency, State, or company resources to assist in response efforts.

Representatives of the Cyber UCG may vary in seniority and position within each organization. Organizations will need to decide what position(s) or individual(s) might serve as a Cyber UCG Senior Official based on the above criteria and the skill sets needed to effectively execute the organization's resources and authorities in coordination with the NCCIC.

During steady state, Senior Officials meet no less than four times a year with the support of Cyber UCG Staff. DHS is the Executive Agent of the Cyber UCG, and the Assistant Secretary for CS&C will chair the Cyber UCG Senior Officials.[27]

Interagency Support to the NCCIC

Cyber Unified Coordination Group Staff

The Cyber UCG Staff exists primarily to synchronize interagency and inter-organization activities between steady state and cyber incident response. Cyber UCG Staff assists the NCCIC Director, Assistant Secretary for CS&C, and Cyber UCG Senior Officials selected for the Cyber UCG Incident Management Team (described in Section 3.2) in carrying out their responsibilities during a Significant Cyber Incident. Cyber UCG Staff will include one representative from the organization of each Senior Official and additional representatives chosen by the DHS Assistant Secretary for CS&C, in consultation with Senior Officials from DOD, DOJ, the FBI, and DOS.

During steady-state, the Cyber UCG Staff serve a liaison function[28] and meet on a monthly basis (at minimum). They are responsible for continuously harmonizing and synchronizing cyber operations, policies, and procedures related to cyber incident response activities as outlined in the NCIRP and in coordination with the varying operational representatives at the NCCIC. Cyber UCG Staff are responsible for keeping Cyber UCG Senior Officials current on NCCIC activities; the overall cyber threat, vulnerability, and consequences picture; and steady-state incident response coordination.

---

[25] UCG Senior Officials may participate virtually if doing so allows them to be more beneficial to the response effort.

[26] Federal agencies should consider designating as the Cyber UCG Senior Official a person who is a properly appointed 'officer' within the meaning of the Appointments Clause in order to ensure that that person may exercise significant authority on behalf of his or her agency.

[27] DHS will provide training to support the UCG Senior Officials and Staff.

[28] They are employed by their home department, agency, or organization and work primarily within their home organization.

NCCIC Support Staff

Full-time support for the NCCIC is provided primarily by elements of the DHS National Protection and Programs Directorate (NPPD). Other elements of DHS,[29] DOD, DOJ, the FBI, NSA, DOS, and other NCCIC partners may provide full-time support as well, including operations staff and liaisons.

NCCIC support staff will work with UCG Staff to provide advice and assistance to the Cyber UCG IMT in the following areas: technical impact, response and recovery recommendations, legal authorities, policy recommendations (including dispute resolution elevation procedures), intelligence and law enforcement, international outreach, and external affairs. All of these staff support functions are available to support NCCIC partners during steady-state operations.

Structure

The NCCIC is designed to evolve to meet the needs of the national cybersecurity and communications CIKR protection and response community. The NCCIC will evolve over time to meet the needs of the partners co-located and virtually connected to the NCCIC, and it will be organized to support the NIMS Incident Command System to provide a full-time structure with the flexibility to scale to manage complex incidents.[30]

The NCCIC Director, under the direction of the Assistant Secretary for CS&C, is responsible for maintaining an appropriately staffed and organized Operations Group, Watch and Warning Group, Analysis Group, Planning Group, Assist and Assess (Logistics) Group, and Liaison Group. Each group will be staffed and organized based on the competencies provided by those participating in NCCIC operations and will be reflected in the NCCIC Concept of Operations (CONOPS).[31] A general description of each group follows.

Operations Group

The Operations Group is responsible for coordinating interagency operational incident management efforts.[32] This responsibility will entail directly coordinating with and integrating information from the various cybersecurity centers, network operations centers, security operations sectors, and other operational entities. Operational execution on different aspects of the response effort will vary based on capabilities, jurisdictional involvement, statutory authority, and priorities set in the incident action plan. The Operations Group ensures the synchronization of these efforts takes place in a manner that ensures the appropriate protection of sensitive information.

Watch and Warning Group

The Watch and Warning Group is the central point for receiving all information that comes to the NCCIC from outside the Operations Group. The Watch and Warning Group is responsible for fusing information from the Operations Group with outside information, maintaining the common operational picture, and executing the NCRAL system. It determines if the incoming information has been previously reported, prioritizes the information, and shares the information

---

29 The Office of Operations and Coordination (OPS), FEMA, I&A, Office of Intergovernmental Affairs (IGA), U.S. Coast Guard (USCG), and USSS.

30 The structure described in the NCIRP may provide assistance beyond Significant Cyber Incidents. For example, the NCCIC may also request partner support for the execution of ESF #2.

31 For example, one ISAC may be most appropriately placed in the Liaison Group based on its charter and capabilities, and another ISAC may have capabilities that would be more appropriately placed in the Watch and Warning Group. For more information on the NCCIC's organization and staffing, see the NCCIC CONOPS.

32 Coordination of operational incident management efforts refers to coordination and situational awareness of overall incident management activities. It does not refer to DHS directing or executing other agencies' responsibilities.

in accordance with standard procedures. The Group also disseminates intelligence products and situation reports at appropriate levels of detail and classification within the NCCIC to the Cyber UCG and appropriate external partners.

Analysis Group

The Analysis Group is responsible for taking the common operational picture and focusing on long-term, strategic, and emerging threats to help inform the NCCIC operating environment and decision makers. This responsibility includes fusing information on past incidents and from a variety of sources with information specific to the threat, incident, or event. The Analysis Group also works with I&A and other partners to generate information and intelligence requirements for ongoing NCCIC operations.

Planning Group

The Planning Group is responsible for developing all operational plans for the NCCIC in coordination with the other groups and the UCG. This responsibility includes developing playbooks and other scenario- and capabilities-based operational plans. Sector-specific plans and procedures for information sharing and coordination will be conducted in concert with the DHS Office of Infrastructure Protection (IP) and other SSAs.

The Planning Group is also responsible for maintaining awareness of the capabilities of all NCCIC partners, preparing and documenting available partner support actions and capabilities, and ensuring strategic and policy collaboration and integration across the cybersecurity centers.

Assist and Assess (Logistics) Group

The Assist and Assess (Logistics) Group coordinates the deployment, distribution, and management of physical personnel deployment or on-site technical assistance. This responsibility includes management of and accountability for Federal supplies and equipment; resource ordering; and delivery of equipment, supplies, people, and services to any assistance efforts outside of the NCCIC operating environment. This Group also assists with ESF #2 logistics activities as needed.

Liaison Group

Elements that operate within the NCCIC provide subject matter expert liaison officers. Liaisons serve as the points of contact for assisting and coordinating activities with various agencies and groups, including SSAs and private sector companies not participating in the Operations Group. For example, an Infrastructure Liaison designated by DHS IP maintains connectivity to the NICC and coordinates with the NCCIC Director to provide advice to the Director and the Cyber UCG regarding issues related to CIKR sectors. The NCCIC also supports other centers with a liaison, such as the DHS CAT, when the Secretary activates it. Cyber UCG Staff will coordinate activities as part of the Liaison Group during steady state.

In coordination with the other groups, the Liaison Group will also work with the originators of information to ensure information can be shared as widely as possible and at different levels of classification and sensitivity.

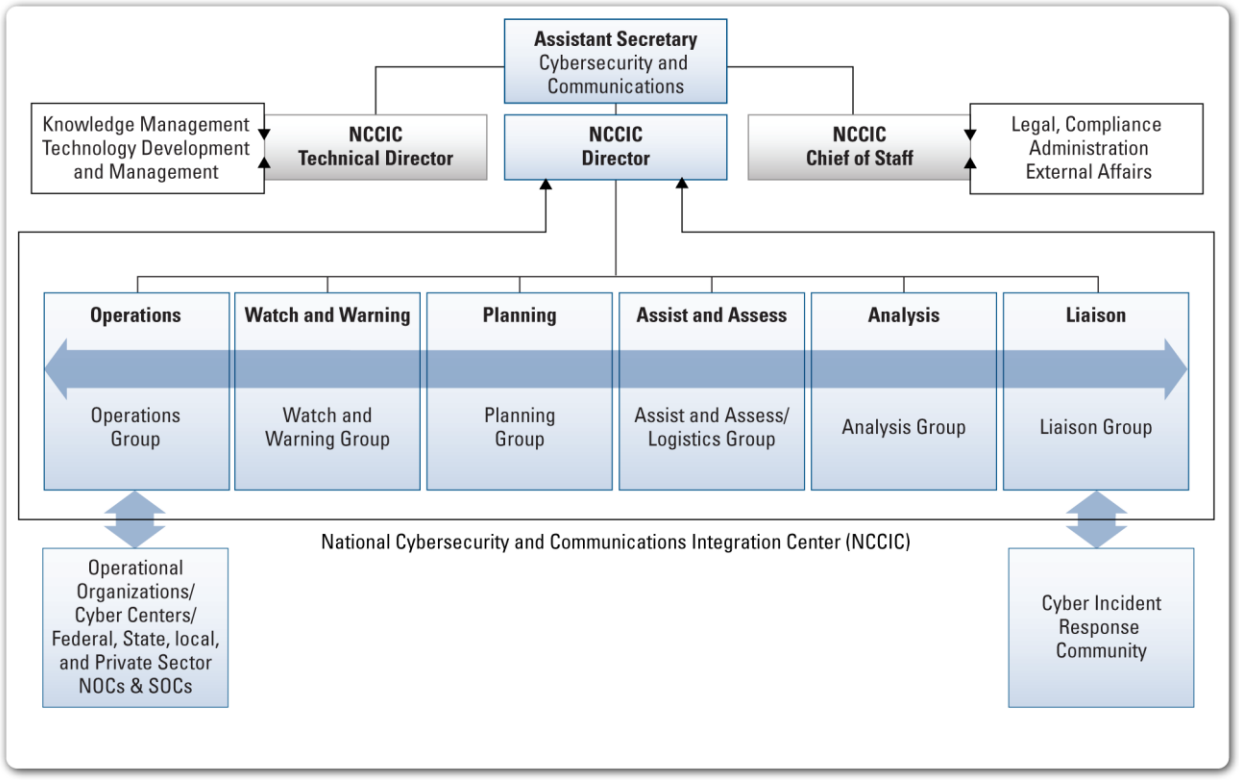


Figure 3: NCCIC Organization, Steady-State

Information Sharing Environment

DHS, through the NCCIC, works on an ongoing basis to identify and integrate appropriate information sharing and collaboration mechanisms. The NCCIC maintains a secure, redundant, and trusted information sharing environment utilizing controlled communications mechanisms[33] where Federal, State, Local, Tribal, and Territorial governments and private sector partners can exchange information consistent with law. This information exchange is based on established information sharing agreements and, where needed and agreed to by the originator of the information, ad-hoc arrangements. DHS will work with the owners and originators of information to ensure the information is shared at the appropriate level of detail and only with the appropriate personnel and organizations after any required equity reviews.

To facilitate this, the NCCIC will have processes in place for protecting information from unauthorized disclosure, including an expedited certification of Protected Critical Infrastructure Information (PCII) and coordination mechanisms to facilitate rapid equity reviews.[34] The Assistant Secretary for CS&C, through the NCCIC Director, is responsible for maintaining the conditions under which sensitive information, including proprietary data, is properly safeguarded.

[33] "Controlled communications mechanisms" refers to real-time, managed information sharing tools, including conference bridges, web tools, and other means to communicate in a trusted environment.

[34] The PCII Program, part of DHS NPPD, is an information protection program that encourages information sharing between the private sector and the Government. Properly certified critical infrastructure information (CII) voluntarily submitted by the private sector can receive protection from Freedom of Information Act disclosure, protection from state and local disclosure laws, protection from use in civil litigation, and protection from use for regulatory action.

Reporting into the NCCIC

During steady state, reporting to the NCCIC can occur in two ways: directly or through previously established reporting chains. Figure 4 depicts "normal" incident reporting for an affected organization as outlined in NIST Special Publication 800-61, *Computer Security Incident Handling Guide, Revision 1.*

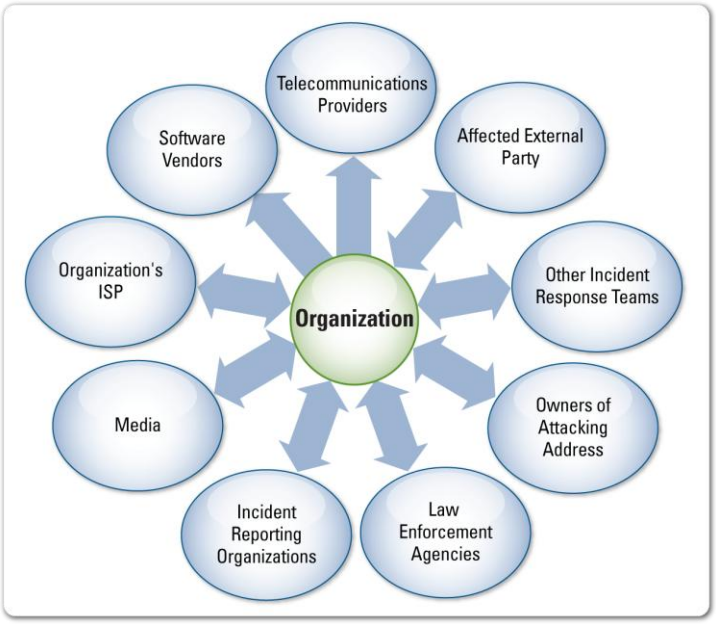


Figure 4: Incident Reporting in NIST SP 800-61

The organization at the center of Figure 4 represents the organization reporting an incident. Depending on the type of organization affected, reporting may occur to a variety of the outlying organizations. By comparison, Figure 5 represents how information would reach the NCCIC through these "normal" incident reporting channels.

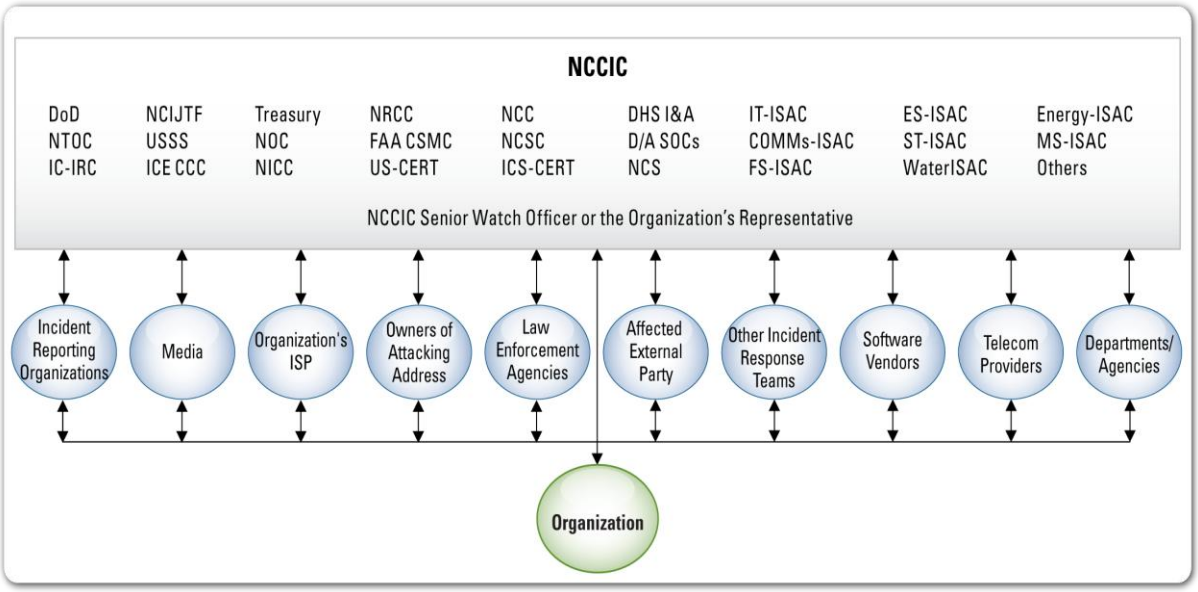


Figure 5: NCCIC Incident Reporting

As depicted in Figure 5, organizations reporting an incident can report directly to the NCCIC through its co-located organizations; indirectly through NCCIC partners, including law enforcement, intelligence, or regulatory agencies; or through ISACs in the form of ISAC analytical information.[35]

For example, information reported through law enforcement channels might reach the NCCIC through the NCIJTF, USSS, the FBI or through direct reporting to the NCCIC by the affected organization. In addition, an organization that chooses to report incident-related information through its telecommunications provider or ISP might reach the NCCIC through the telecommunications provider directly or through the reporting of the NCC/communications sector ISAC. Building on Figure 5, these scenarios are graphically depicted in Figure 6 and Figure 7.

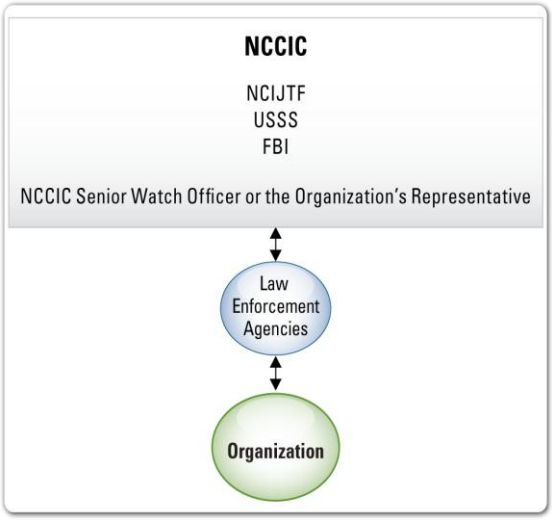


Figure 6

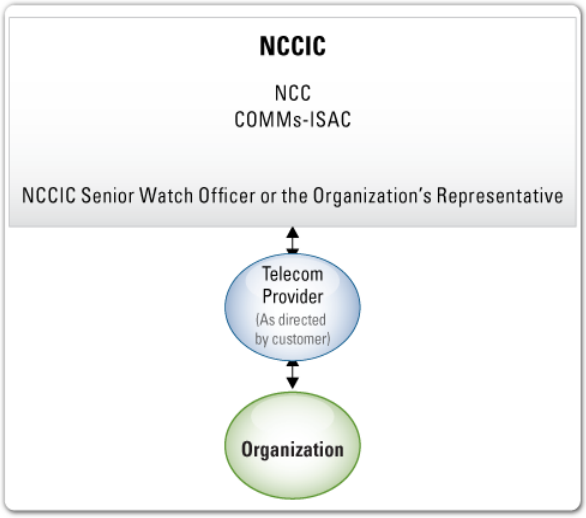


Figure 7

Organizations without formal, established reporting mechanisms or without 24x7 channels through which to report information may prefer to communicate directly with the NCCIC.[36] Those with other formal information sharing relationships are similarly encouraged to continue these relationships.

3.2 ORGANIZATION DURING A SIGNIFICANT CYBER INCIDENT

Because the Federal Government and its cybersecurity partners have learned that regular communication and interaction before an incident strengthens relationships and helps clarify incident response roles, it is essential that these relationships are leveraged during a Significant Cyber Incident. At Level 2 or Level 1 of the NCRAL system, the NCCIC scales from steady-state operations to meet incident objectives effectively by including all partners and Cyber UCG Senior Officials needed to execute effective incident response and risk mitigation activities.

NCICC

As the central national point of coordination for day-to-day cyber response efforts, the NCCIC is in a unique position to facilitate domestic incident management for Significant Cyber Incidents

[35] As depicted in Figure 5, ISACs are represented as incident reporting organizations, but many provide extensive services beyond incident reporting.

[36] Reporting to the NCCIC is not a substitute for any reporting required by law, regulation, or prior agreement.

that require a coordinated national response. Therefore, the NCCIC remains the platform for coordinating operational response activities, including incident prioritization, critical resource allocation, and situational awareness for Significant Cyber Incidents. This coordination includes communicating cyber incident-related situational awareness to NCCIC partners, the Secretary of Homeland Security, and the White House and coordinating with the NOC, NICC, and NRCC to monitor and prepare for the possible onset of any physical consequences.

If needed partners are not present during the onset of a Significant Cyber Incident, the NCCIC maintains the capability to physically or virtually add additional Federal, State, Local, Tribal, Territorial, and private sector partners, including international stakeholders as appropriate, to the coordinated NCCIC effort. Affected partners, and those that can contribute to the response effort and risk mitigation activities, can be physically co-located and virtually connected to coordinate Significant Cyber Incident response efforts.[37]

Leadership

Assistant Secretary for CS&C

During a Significant Cyber Incident, the Assistant Secretary for CS&C reports directly to the Secretary of Homeland Security, serves as the National Cyber Incident Manager, and is responsible for coordinating all Significant Cyber Incident-related activities for the Secretary of Homeland Security.[38] During a Significant Cyber Incident at Level 2 or Level 1, the Assistant Secretary for CS&C focuses primarily on his or her cyber incident management responsibilities. The Assistant Secretary for CS&C coordinates Significant Cyber Incident management activities from the NCCIC in concert with the Cyber UCG IMT. The Assistant Secretary for CS&C, through the NCCIC Director, will have established procedures in place to notify the Secretary, NPPD leadership, all Cyber UCG Senior Officials, the NICC, the NOC, and the White House Cybersecurity Coordinator of the status during each response phase.[39] The Assistant Secretary for CS&C is responsible for coordinating with the Manager of the NCS, especially in situations related to the degradation or disruption of communications infrastructure.[40]

If the President or Congress authorizes military action to defend the United States, and if the President, as Commander in Chief, determines that the Secretary of Defense should provide leadership for incident management, the Assistant Secretary for CS&C, through the Secretary of Homeland Security, will work through NCCIC processes and procedures to support the Secretary of Defense's incident management efforts.

Cyber UCG IMT

Because needed resources, authorities, and execution responsibilities do not reside in one department, agency, organization, or company, the Assistant Secretary for CS&C coordinates cyber incident response efforts from the NCCIC with the help of the Cyber UCG IMT. The Cyber UCG IMT consists of selected Cyber UCG Senior Officials who can quickly bring

[37] The Assistant Secretary, in coordination with the Cyber UCG IMT, will be responsible for ensuring the proper individuals are included in this effort and are able to do so in teams, or in coordinated groups as needed, while ensuring propriety information can remain safeguarded.

[38] This does not prohibit the Secretary from choosing another Cyber Incident Manager based on the nature of the incident and operational roles and competencies.

[39] This does not preclude any department or agency from directly notifying the White House Cybersecurity Coordinator of the status of its response efforts. The NCCIC also provides information to the DHS Chief Privacy Officer in accordance with the provisions of the Privacy Act and related laws and policies.

[40] The Manager of NCS is responsible for managing the coordination of, planning for, and provision of national security and emergency preparedness communications for the Federal Government under all circumstances.

together needed resources, authorities, and information for a common situational awareness to respond to a Significant Cyber Incident. Participants in the Cyber UCG IMT utilize their own authorities and execution responsibilities to assist response activities and are responsible for understanding and communicating the full range of response capabilities that their agency or organization brings to bear.

The exact composition of the Cyber UCG IMT will be determined by the Assistant Secretary for CS&C based on the nature and scope of the incident, and will always include—

- A Senior Defense Official
- A Senior Federal Law Enforcement Official[41]
- A Senior IC Official
- Senior Private Sector Official(s) (chosen based on the specific nature of the incident)
- Other Cyber UCG Senior Officials with primary statutory or jurisdictional responsibility and significant operational responsibility chosen based on the nature of the incident; Senior Officials may be chosen from departments, agencies, and organizations with capabilities, authorities, and responsibilities relevant to the incident.

Each department and agency involved in a Significant Cyber Incident shall be responsible for ensuring the availability of its Senior Official to the Cyber UCG IMT. Senior Officials should have familiarity with the incident and the NCCIC based on coordination with the Cyber UCG Staff and, ideally, will be familiar to NCCIC partners. The Cyber UCG IMT will jointly determine objectives, plans, and priorities for the incident action plan and will work together to execute the plan.

The Assistant Secretary for CS&C, with the support of the NCCIC and in concert with the Cyber UCG IMT, is responsible for—

- Establishing the incident action plan
- Ensuring overall coordination of Significant Cyber Incident management and resource allocation activities
- Facilitating interagency conflict resolution or elevating matters, as necessary
- Coordinating response between multiple cyber incidents when applicable
- Ensuring the NOC and NICC receive timely updates on the status of response activities
- Coordinating external affairs activities.

As during steady state, a wide variety of critical international relationships will be individually managed by key partners to ensure that they maintain and adhere to their international agreements, where applicable. DOS works with the NCCIC and all relevant departments and agencies to facilitate multilateral and bilateral coordination efforts as needed during a Significant Cyber Incident. The Assistant Secretary for CS&C and the Cyber UCG IMT will work through the NCCIC to coordinate and deconflict direct international engagements.

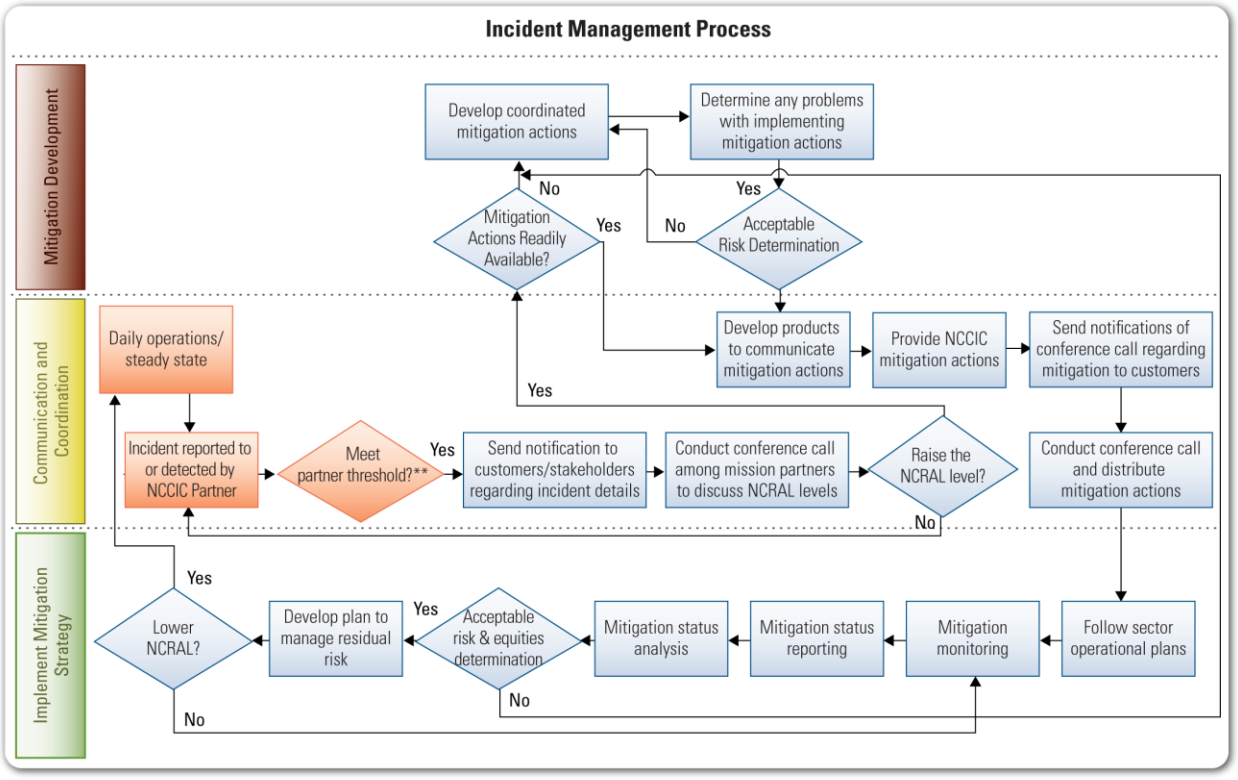
All members of the Cyber UCG IMT will be invited to meet physically at the NCCIC to assist with coordination efforts. Some members may participate in the Cyber UCG IMT virtually if doing so allows them to be more beneficial to the response from their home organization. The

[41] The Senior Federal Law Enforcement Official (SFLEO) is appointed by the Attorney General during an incident requiring a coordinated Federal response to coordinate all law enforcement, public safety, and security operations with intelligence/investigative law enforcement operations directly related to the incident.

Cyber UCG IMT will stand down when the goals outlined in the incident action plan have been achieved and the NCRAL system is lowered to Level 3.

Process

The NCCIC Director and Staff work with the Cyber UCG Staff to present recommendations and associated risks to the Assistant Secretary for CS&C and the Cyber UCG IMT for coordination and execution in accordance with the NCCIC incident management process (see Figure 8).



** The term "partner" refers to public and private sector partners including cybersecurity centers. The term "threshold" refers to the agreed upon types of threats/vulnerabilities for notification (i.e., criminal acts, threat investigation, etc.) to partners and DHS Leadership.

*** The blue boxes indicate processes that the UCG IMT help coordinate during a significant Cyber Incident.

Figure 8: NCCIC Incident Management Process

In addition, the NCCIC External Affairs Officer is responsible for working with the Assistant Secretary for CS&C, Cyber UCG, DHS Office of Public Affairs, White House Communications, Public Information Officers, and National Joint Information Center (NJIC) to create and maintain communications plans associated with the NCIRP and to manage external affairs and ESF #15 activities, as needed or required. The External Affairs Officer will work to integrate public affairs, congressional affairs, and intergovernmental affairs into external affairs efforts; utilize pre-identified communications protocols during a Significant Cyber Incident; and formulate the public affairs incident action plan to guide messaging to public and external stakeholders. Whenever possible, public information officials from all participating agencies and organizations should coordinate closely with the NCCIC and NJIC.

4 ACTIONS OF THE INCIDENT RESPONSE CYCLE

The actions depicted in Figure 9 and described in the following sections are based on phases of the incident response cycle and should be conducted in partnership with cyber incident response partners at the NCCIC.

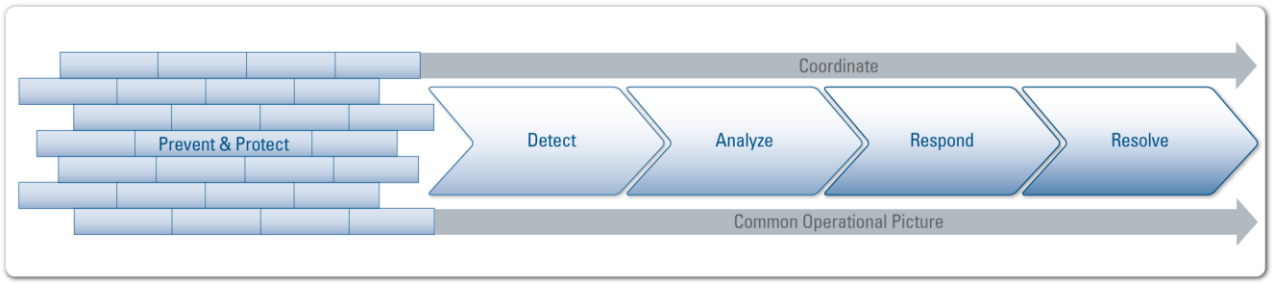


Figure 9: Cyber Incident Response Cycle

4.1 COORDINATION AND THE COMMON OPERATIONAL PICTURE

Coordination and the development of the common operational picture are fundamental elements of prevention and protection activities and are especially essential during detection, analysis, response, and resolution activities. The steady-state relationships developed at the NCCIC should assist coordination during all phases of the incident response cycle and during all levels of cyber risk. However, during a Significant Cyber Incident, coordination is especially important because each partner organization may have different priorities and drivers for its decisions. A CIKR owner and operator may be focused on containment and recovery, while Federal partners may be focused on attribution and prosecution. Having the national common operational picture in mind, the NCCIC is in a unique position to assist in the deconfliction of these priorities and to work with other departments and agencies with specific deconfliction authorities.[42]

The information sharing environment established among NCCIC partners facilitates the development and maintenance of a common operational picture throughout the incident response cycle and provides the foundation for successful response efforts. NCCIC partners develop and share tips, indicators, warnings, information, and mitigation recommendations using established communications channels. Although constant steady-state communication is planned, regular communication may need to increase in scope and detail based on the NCRAL system levels.

The NCCIC, as the national focal point for cyber incident management and coordination during cyber-specific incidents, is the point of integration for all information from Federal departments and agencies, State Local, Tribal, and Territorial governments, and the private sector related to situational awareness, vulnerabilities, intrusions, incidents, and mitigation activities.[43]

[42] In accordance with the escalation procedures developed by the UCG.

[43] This role does not change existing departments' and agencies' authorities or missions; however, DHS, through the NCCIC, will coordinate with all partners, including law enforcement agencies leading the national effort to investigate and prosecute cybercrime; the IC regarding threats, intelligence, and attribution; DOD elements regarding intelligence and information sharing, military operations to defend the homeland; State and Local governments; and the private sector to ensure common operational situational awareness is being leveraged by all response organizations as they execute their individual authorities and missions.

4.2 PREVENT AND PROTECT

The public and private sector participants at the NCCIC continually monitor and track threats, vulnerabilities, disruptions, and intrusions to help prevent and protect critical cyber infrastructure. The NCCIC makes indications and warning information available to all relevant organizations to highlight the emergence of critical changes in the overall state of U.S. cyber infrastructure. Organizations within the NCCIC work to ensure the NCCIC and other critical partners receive and are able to act on preventative and protective information throughout all phases of the incident response cycle.

4.3 DETECT

When prevention and protection efforts are unsuccessful, Federal, State, Local, Tribal, Territorial and private sector owners and operators of critical networks are likely to be the first to detect malicious or unauthorized activity on their networks. These owners and operators work individually within their incident response processes and, when appropriate, in partnership with others to identify and contain malicious and unauthorized activity on critical networks. They seek to gather as much information as possible on the unauthorized activity, including any critical details on the "who, what, where, when, why, and how" of the incident, if known. In addition, when available, information on threats and vulnerabilities from a variety of sources may be made available via the NCCIC to appropriate response partners. Similarly, information from the IC may be available at the appropriate level of classification in order to assist with detection activities across critical networks.

Based on this network detection and information gathering activity, each organization works to determine risks and operational impacts based on further analysis and/or two-way communication with the NCCIC, sector-designated organization, or other incident partners.

4.4 ANALYZE

Analysis of an incident is conducted to discover whether an incident was malicious or unintentional and to assess its impact, scope, and severity. Analysis is an ongoing process that takes into account detected activity over time and adjusts accordingly. Analysis should incorporate data and information from multiple sources whenever possible and should be conducted and communicated in the overall context of the NCRAL system.

Many organizations have robust analytical activities underway. Each organization may conduct its own assessment and collaborate with others but is encouraged to share information on the potential incident with the NCCIC or any of its participating organizations. Analysis should include the technical aspects of the incident, mission or business impact, and visibility and public affairs impact.

The NCCIC brings together data from a wide variety of information sources to help with further analysis, build a robust common operational picture, and conduct further analysis to determine the NCRAL system alert level. The NCCIC works with partners to characterize and prioritize incidents based on risk to the Nation's cyber infrastructure, economic and national security, public confidence, and the public's health and safety.

4.5 RESPOND

Response activities happen within organizations every day and can be conducted with the assistance of NCCIC partners upon request or by mutual agreement. During coordinated

operations at Levels 2 and Levels 1 of the NCRAL system, the Assistant Secretary for CS&C coordinates response efforts from the NCCIC with the Cyber UCG IMT, including determining the incident action plan, evaluating the effectiveness of the response, and adjusting the effort based on the goals of the incident action plan.

Each organization involved in a Significant Cyber Incident plays a unique response role because each has a distinct mission and different authorities. Needed response resources should be readily available and based on each organization's cyber response plans and authorities. Responsibilities include notifying and activating cyber response organizations, plans, and personnel; requesting assistance when needed; and initiating or continuing law enforcement investigations. The NCIJTF coordinates cyber investigations in partnership with other elements of the intelligence and law enforcement communities. Information relevant to protection, mitigation, threats, and vulnerabilities will be reported, where permitted by law, to the Assistant Secretary for CS&C and the Director of the NCCIC. The NCCIC notifies the appropriate stakeholders of the situation and will continue to coordinate required and requested response activities according to established operational tempos.

Requests from NCCIC for assistance from partners or sectors that lack the capacity to respond on their own are coordinated through the NCCIC and prioritized and assigned to responding agencies based on direction from the Cyber UCG.

It is possible that, because of response activities, the Assistant Secretary for CS&C may adjust the NCRAL system to a lower level. The coordinated response effort and the work of the Cyber UCG IMT terminates when the goals, strategies, and intended outcomes outlined in the incident action plan are met and with concurrence of the Assistant Secretary for CS&C.

4.6 RESOLVE

The Assistant Secretary for CS&C and the Cyber UCG IMT work to confirm that the intended outcomes of the response effort have been met or that response efforts can be successfully managed without national coordination.

The Assistant Secretary for CS&C works with the NCCIC Director and the Cyber UCG Staff to issue appropriate advisories and communications.

The Assistant Secretary for CS&C, Cyber UCG IMT members, and Cyber UCG Staff collect lessons learned from the incident and organize and participate in lessons learned activities. Cyber UCG Staff work to coordinate the implementation of long-term corrective actions by monitoring, tracking, and measuring their implementation.

5 UNIVERSAL ROLES AND RESPONSIBILITIES

The following is intended to assist all entities with understanding their general roles and responsibilities for preparedness, response, and short-term recovery during a cyber incident.

5.1 PREPAREDNESS

Preparedness activities, including establishing common situational awareness in a common operational picture, are shared responsibilities across Federal, State, Local, Tribal, and Territorial governments and the private sector. By the time coordinated response actions are needed during a Significant Cyber Incident, the cybersecurity community must be prepared and maintain a shared situational awareness to help identify, respond to, and recover from an incident.

In all phases of the incident lifecycle, it is essential for each Federal, State, Local, Tribal, and Territorial government and private sector partner to have its own means of establishing its situational awareness and a trusted means by which to share information to help establish a well-integrated national common operational picture. The NCCIC will provide the mechanisms and facility to allow for the development of a common operational picture in accordance with the NCCIC CONOPS. Because situational awareness is only as good as the participation and input provided by partners in the NCCIC and others, the NCCIC collaborates in accordance with standing information sharing agreements among NCCIC partners.

Preparedness is a basic responsibility of all Federal, State, Local, Tribal, Territorial, and private sector organizations. Each organization plays a unique role in preparing for a cyber incident with respect to its distinct mission and authorities. All organizations are responsible for the following preparedness activities:

Engage:

- Engage with the NCCIC, sector-designated operational organizations such as ISACs, and other organizations within the cyber incident response community.

Plan:

- Maintain incident response plans that align with the most current version of the NCIRP.
- Adopt policies, make plans, outline procedures, and enact agreements that are aligned with the NCIRP. These policies, plans, procedures and agreements should allow each organization to perform essential tasks during a cyber incident and to coordinate with the NCCIC and other response partners.
- Assess "lessons learned" from previous incidents and exercises and incorporate these lessons into preparedness activities and plans.
- Identify, assess, and manage risks to mission-critical infrastructure and critical infrastructure generally.
- Engage with NCCIC partners, including sector-designated operational entities such as ISACs, to facilitate sector-specific information sharing activities.

Organize:

- Develop pre-scripted cyber incident assignments and keep them updated.
- Engage in Advanced Readiness Contracting to ensure contracts are in place for common commodities and services that may be needed during a cyber incident, including mission-critical items such as critical spares and necessary hardware and software; use secure supply chain procurement and key practices for supply chain and overall risk management.
- As needed, ensure resources are pre-positioned to assist with common response activities and mission-critical items.
- Identify network entry points, system interdependencies, and network topology mapping.

Equip:

- Ensure facilities, systems, supplies, and personnel are prepared for and ready to respond in an incident.
- Identify critical assets, systems, networks, and functions and manage risk to these systems.
- Make regular system backups in case system restoration is needed.

Train:

- Ensure individuals, teams, and organizations are trained in cyber incident response procedures, including internal and external reporting mechanisms.
- Ensure that organizational structures and leadership that will be participating in incident response activities (including Senior Officials) are trained and familiar with the NCIRP, NRF, and NIMS.
- Ensure individuals meet professional qualifications and performance standards and have been trained in their specific role (if any) under the NCIRP or their organization's plan.

Exercise:

- Exercise cyber-specific incident response and recovery plans, including for cyber incidents that have physical consequences.
- Participate in and document the results of multi jurisdictional exercise programs that have a cyber component and share these results as appropriate.

Evaluate and Improve:

- Include mechanisms to capture lessons learned from exercises and incidents.
- Institute corrective actions from the lessons learned from exercises and real-world incidents.
- Provide a method for reporting information related to the global supply chain that will be critical to after-action reports, future incidents, and information sharing capabilities across the government and the private sector.

5.2 CYBER INCIDENT RESPONSE

Each organization involved in a cyber incident will play a unique response role. Each has a distinct mission and different authorities, so response actions will differ. However, all partners in the NCIRP have the responsibility to maintain, at minimum, the following capabilities during the response phase:

All organizations should have the ability to gain and maintain situational awareness about the performance of any unauthorized activity on their networks and communications systems.

Information based on this awareness should be passed to the NCCIC directly or through previously established reporting channels to help inform the national picture. DHS, through regular communications and implementation of the NCRAL system, will assist organizations in ensuring that they understand what type of information needs to be shared throughout the incident response cycle.

Necessary response resources should be readily available and should be based on each organization's cyber response plans as informed by the NCIRP. This includes notifying and activating cyber response organizations, plans, and personnel and requesting assistance when needed. All departments, agencies, and organizations should notify pre-identified Cyber UCG Staff and Cyber UCG Senior Officials and make them available to the NCCIC and/or other operations centers as needed upon request of the Assistant Secretary for CS&C. In addition, staff may need to be deployed for physical patching and/or repair.

During the course of the incident, organizations that may have responded under their own authorities should notify the NCCIC and coordinate further actions as part of the national response effort. Once the NCCIC receives additional reporting, it notifies appropriate cyber

incident stakeholders of the situation and continues to coordinate required and requested response activities.

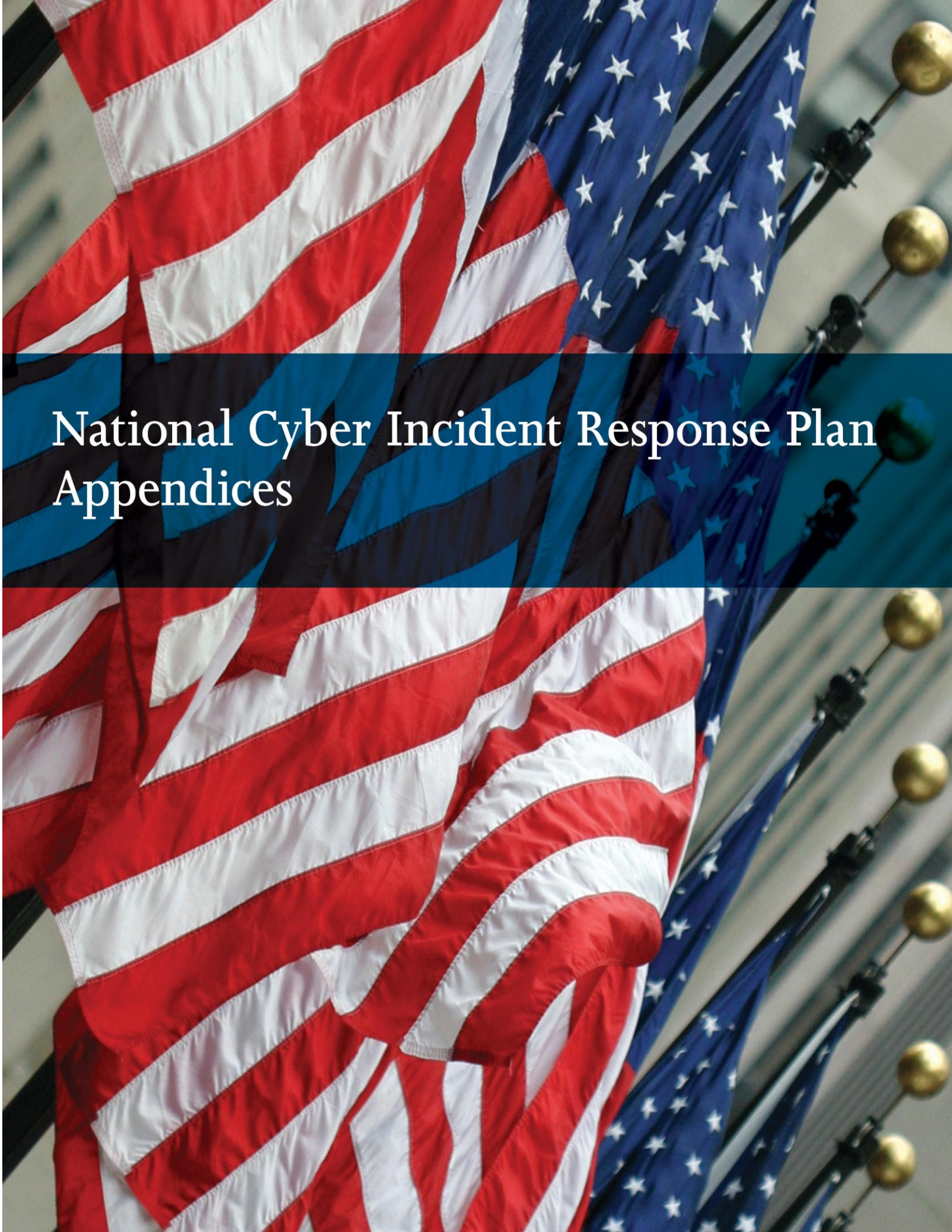
5.3 SHORT-TERM RECOVERY[44]

Consistent with the NRF, short-term recovery begins immediately after the incident and may overlap with response efforts. It includes providing and restoring essential services. As with the response effort, each organization plays a unique role in recovering from a cyber incident. All partners in the NCIRP should take the following common recovery actions during the short-term recovery phase:

- Continue to maintain and report situational awareness to the NCCIC and other designated operational entities.
- Assist in analyzing and addressing the "root cause" of the incident.
- Reassess or assist in reassessing information and communications technology architecture to ensure it is no longer systemically vulnerable and that the problem has been accurately located.
- Continue to work within existing missions to ensure service continuation or service restoration to facilitate performance of operational roles.
- When necessary, reallocate resources from less vital missions to provide additional recovery capability.
- When necessary, reevaluate thresholds if operating at less than normal capability.
- Provide technical expertise to assist in the restoration of essential services.
- Assess damages caused by the incident.
- Assess "lessons learned" from the cyber incident and incorporate these back into the preparedness and response phases.

[44] Short-term recovery begins immediately and can overlap with response. It includes providing and restoring essential services. Long-term recovery is outside the scope of the NCIRP (and NRF). Although it involves many of the same actions, it may continue for months and years.

[This page intentionally left blank.]



National Cyber Incident Response Plan Appendices

[This page intentionally left blank.]

Appendix A: National Response Framework Cyber Incident Annex (National Cyber Incident Response Plan Quick Reference Guide)

[This page intentionally left blank.]

[Reserved for final NCIRP language summarized and presented in the NRF Incident Annex format - to be added after Cyber Storm III]

[This page intentionally left blank.]

Appendix B: Department of Homeland Security Roles and Responsibilities

Preparedness

The Department of Homeland Security (DHS) has preparedness responsibilities as the national coordinator for Significant Cyber Incident response, in addition to specific responsibilities to the Federal Government, State and Local governments, and the private sector.

At the *national* level, DHS works with its Federal, State, Local, Tribal, Territorial and private sector partners to establish and maintain nationally integrated cybersecurity and communications situational awareness. At the National Cybersecurity and Communications Integration Center (NCCIC), DHS integrates incident information from across the Federal Civilian Enterprise (.gov), .mil, and Intelligence Community (IC) networks; State and Local domains; law enforcement; and critical private sector networks that have volunteered information to be shared.

As part of this responsibility, DHS continuously works to establish, refine, and maintain a trusted information sharing environment utilizing controlled communications mechanisms where Federal, State, Local, Tribal, and Territorial governments and private sector partners can share information. This environment allows for the sharing and receiving of threat and vulnerability information with the public and the private sectors.

DHS, utilizing available resources and partnerships at the NCCIC, prepares to serve as the national focal point for Significant Cyber Incident management and coordination during cyber-specific incidents. This responsibility includes responding to steady-state incidents that are part of the daily operational tempo, as well as preparing to respond to catastrophic incidents that could degrade or overwhelm the networks, systems, and assets that operate the Nation's information technology (IT) and communications infrastructure. As part of this preparation and pursuant to the responsibilities outlined in Homeland Security Presidential Directive 5 (HSPD-5) and HSPD-7, the Assistant Secretary for the Office of Cybersecurity and Communications (CS&C) serves as cyber incident manager. The NCCIC ensures core Federal, State, Local, Tribal, Territorial, and private sector participants can be physically or virtually co-located during an incident to help manage and lead the response to a Significant Cyber Incident. This responsibility includes sponsoring national security clearances, ensuring access to the NCCIC for essential personnel, and ensuring participants have access to their home organizations' IT systems to the greatest extent practicable.

The NCCIC contains operational elements from many key partners. DHS works with Cyber Unified Coordination Group (UCG) Staff to prepare to host the Cyber UCG Incident Management Team (IMT) to assist the Assistant Secretary for CS&C and the NCCIC Director in coordinating decision making and resource allocation among cyber incident response partners. The Cyber UCG Staff works to prepare harmonizing response policies and provide strategic guidance and direction to ensure a smooth transition during a Significant Cyber Incident.

Physical co-location may not be an option for some essential decision makers during an incident. DHS, therefore, works with its partners across Federal, State, Local, Tribal, and Territorial governments and the private sector to ensure robust communications and provide incident-specific access to other facilities that maintain secure communications mechanisms. This effort ensures virtual co-location can be effectively implemented and communication can occur during a cyber incident.

In addition, response teams may need physical access to key cyber and communications components during or immediately after a cyber incident. However, if a cyber incident has physical consequences, on-scene response personnel may manage and control site access. The NCCIC works to facilitate Federal, State, Local, Tribal, Territorial, and private sector incident response activities by ensuring mechanisms to allow incident site access are in place.

DHS also works with critical partners to coordinate preparedness activities, exercises, lessons learned, and best practices for those who wish to participate and for those unable to develop these elements on their own. This coordination includes integrating the lessons learned from exercises into plans and everyday activities.

At the *Federal* level, in cooperation with Federal departments and agencies and, by request, with Legislative and Judicial Branch organizations, DHS establishes and maintains shared situational awareness across Federal civilian departments and agencies' .gov space. This effort includes receiving reports on and analyzing intrusions and incidents across departments and agencies on a 24x7 basis and partnering with Federal departments and agencies to develop proactive approaches to improving security and managing cyber risk to U.S. networks. DHS similarly works to integrate information from the Federal cybersecurity centers. As required, DHS supports other Federal departments and agencies in the execution of their responsibilities. This support may lead to other departments exercising their authorities at the request of DHS or to DHS taking action on behalf of departments requesting assistance.

At the *State and Local* levels, DHS partners with State, Local, Tribal, and Territorial governments and coordinates with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to define what information is useful to establish and maintain national situational awareness. This support includes providing a mechanism for State, Local, Tribal, and Territorial reporting into the MS-ISAC and the NCCIC for establishing and maintaining situational awareness. DHS also partners with State, Local, Tribal, and Territorial governments on improving security, exercising cyber incident response and recovery plans, and, upon request, participating in State, Local, Tribal, and Territorial preparedness activities.

Within the *critical infrastructure and key resources (CIKR)* community, DHS partners with public and private sector CIKR partners to define what information is useful to establish and maintain national situational awareness, including describing information sharing objectives related to situational awareness, analysis, prevention, detection, mitigation, response, and recovery. DHS works with the private sector, including sector-designated operational entities such as ISACs, to explore new ways to improve security and enhance information sharing, including providing appropriate detection and prevention threat signatures to allow the CIKR community to detect and mitigate any attacks internally. DHS works with the CIKR community to provide a clear mechanism for private sector reporting to DHS and ensures mechanisms exist to protect private sector information from unauthorized disclosure, including any proprietary information provided to DHS during steady state or during a Significant Cyber Incident. All agencies in the NCCIC shall ensure that mechanisms exist to provide that information with other government agencies while protecting private sector information.

Upon request, DHS participates in private sector exercises and works with the private sector to assist in exercise development.

At the *international* level, DHS works with other departments and agencies, including the Department of State (DOS) and international partners, to establish and maintain shared

situational awareness, improve security, and plan for cyber incidents that affect the homeland and require an internationally coordinated response. This effort includes working with NCCIC partners to synchronize and deconflict international efforts. DHS works with its Federal partners to maintain situational awareness on foreign cyber threats and, as appropriate, will participate in international exercises.

In general, DHS will work on awareness and education activities to help prepare the U.S. public for a Significant Cyber Incident and will prepare an external affairs plan that aligns with Emergency Support Function -15 (ESF #15) and the National Incident Management System (NIMS) to ensure coordinated public communications during an incident.

Cyber Incident Response

At the national level, the Secretary, as principal Federal official for incident management, coordinates the national response effort for cybersecurity and communications response, recovery, and reconstitution. In the case of disagreement among members of the UCG IMT, the Secretary (likely through the Assistant Secretary for CS&C) provides a mechanism to resolve interagency policy issues or quickly elevate them to the White House National Security Council (NSC) for interagency resolution. In close coordination with the originators of information and with other partners, the NCCIC requests, receives, shares, and analyzes information on attack techniques and vulnerabilities at the lowest level of classification or restriction possible and works with NCCIC partners to mitigate threats to critical networks. DHS also works with law enforcement agencies that are leading the national effort to investigate and prosecute cybercrime. At all levels, DHS, through regular communications and implementation of the National Cyber Risk Alert Level (NCRAL) system, assists organizations in ensuring they understand what type of information needs to be shared throughout the incident response cycle.

At the *Federal* level, the NCCIC works with Federal departments and agencies to lead and coordinate incident response activities across Federal Executive Branch civilian (.gov) networks. Upon request, the NCCIC provides assistance to the Legislative and Judicial Branches.

At the *State and Local* levels, at the request of State, Local, Tribal, and Territorial governments, the NCCIC, in coordination with the MS-ISAC, coordinates and assists with incident response activities on State, Local, Tribal, and Territorial networks. DHS assists, as needed, with State, Local, Tribal, and Territorial participation in response activities virtually or through physical representation at the NCCIC during an incident. DHS coordinates with Chief Executives of State, Local, Tribal, and Territorial governments; their representatives; and the MS-ISAC to maintain situational awareness across State networks.

Within the *private sector* community, DHS shares and receives incident information with private sector partners, including sector-designated operational entities, through appropriately secured calls and e-mails and with private sector representatives at the NCCIC. DHS also collaborates with the private sector to identify additional information sources and coordinates on the collection, analysis, and sharing of such data in real time to help prioritize actions and resource allocation to secure CIKR networks.

DHS leverages the collective capabilities of industry, sector-designated operational entities, and the Government to conduct collaborative analysis on malware and other components of cyber attacks. DHS coordinates outreach across CIKR sectors; determines to what extent information needs to be shared more broadly, in accordance with applicable laws and policies; and identifies and shares protection and remediation actions. DHS also coordinates support for different CIKR

sectors, including analysis and system recovery assistance, to ensure continued availability of the infrastructure.

At the *international* level, DHS, in coordination with DOS, works with international partners, allies, and Computer Security Incident Response Teams to coordinate and synchronize response activities and provide common situational awareness, in accordance with deconflicted procedures established by NCCIC partners.

Short-Term Recovery

At the *national* level, DHS works with other departments and agencies, State Local, Tribal, and Territorial governments, and private sector CIKR to prioritize cyber recovery efforts for critical systems and services. In coordination with the IC, DOD, and the Department of Justice (DOJ), DHS will continue to provide information on ongoing threats and will maintain situational awareness in cooperation with incident partners and victims. DHS coordinates recovery efforts across the .gov network in close cooperation with affected departments and agencies and with the Legislative and Judicial Branches upon request.

Appendix C: Department of Defense Roles and Responsibilities

Preparedness

At the *national* level, the Department of Defense (DOD), in collaboration with the Intelligence Community (IC) and pursuant to applicable law and policy, provides cyber warning capabilities to assist in characterizing cyber incidents. DOD plans and prepares for DOD cyberspace operations and prepares to use cyberspace as a domain to deter, deny, or defeat any adversary seeking to harm U.S. national and economic security. DOD coordinates activities with the Department of Homeland Security (DHS) through existing mechanisms and through virtual or physical representation at the National Cybersecurity and Communications Integration Center (NCCIC).

At the *Federal* level, DOD establishes and maintains shared situational awareness across DOD networks (.mil) and shares that information with Federal partners to ensure that multidirectional information sharing and situational awareness is maintained at the national level within the limits of DOD authority. As required, DOD supports other Federal departments and agencies in the execution of their responsibilities.

DOD coordinates preparedness activities, exercises, and lessons learned for .mil stakeholders and among those who request participation or need assistance from DOD. DOD formulates and implements defense, response, and recovery strategies to assure the availability of the .mil network.

At the *State and Local* levels, DOD supports DHS and the National Guard Bureau and, in preparing Defense Support of Civil Authorities (DSCA), partners with State, Local, Tribal, and Territorial governments to define what information is useful to establish and maintain situational awareness.

Within the *private sector critical infrastructure and key resources (CIKR)* community, DOD works directly with defense industrial base partners, DHS and Sector Specific Agencies (SSA), and other CIKR partners in developing plans to assist in securing specified CIKR information systems. DOD also incorporates Information Assurance (IA) situational awareness into plans and operations for its private sector security partners in coordination with DHS through the National Infrastructure Protection Plan (NIPP) structure. DOD assists in the development and distribution of best practices to be shared with DOD private sector security partners. When directed by the President of the United States (POTUS) or the Secretary of Defense, DOD supports DHS in its efforts to secure CIKR.

At the *international* level, DOD works with other departments and agencies, including the Department of State (DOS) and international partners, to maintain situational awareness about foreign cyber threats. DOD also works with international partners and allies through cooperative security engagements to develop and maintain situational awareness about foreign cyber threats and across military networks.

Cyber Incident Response

At the *national* level, DOD provides representation and leadership support to the Assistant Secretary for the Office of Cybersecurity and Communications (CS&C) in the form of a Cyber Unified Coordination Group (UCG) Senior Official. This Senior Official represents the Secretary

of Defense and works with the Assistant Secretary for CS&C to establish and execute unified and joint priorities and overarching objectives for incident response and recovery.

At the *Federal* level, DOD directs the operation and defense of the .mil network in support of DOD's full spectrum of warfighting, intelligence, counterintelligence, and business missions. DOD, when requested by other Federal entities as appropriate and in close coordination with the NCCIC, can provide technical assistance to gather and analyze information to characterize the attack and to gain attribution of the cyber threat, offer mitigation techniques, perform network intrusion diagnosis, provide technical expertise, and take action to deter or defend against cyber attacks that pose an imminent threat to national security, where authorized by applicable law and policy. DOD provides DSCA when requested. As authorized by applicable law and directed by the President, DOD may be designated the lead Federal agency with other departments or agencies supporting DOD for Significant Cyber Incident response.

At the *State and Local* levels, and when directed by the Secretary of Defense, DOD provides DSCA when requested and, in close coordination with DHS, shares threat information with the State National Guard and other State-level partners in accordance with applicable statutory authorities and established protocols.

Within the *private sector* community, and when directed by the Secretary of Defense, DOD assists its private sector security partners with response activities in close coordination with DHS. DOD also provides cyber incident reporting and analysis information to industry partners under the voluntary and collaborative Defense Industrial Base (DIB) Cybersecurity/IA program.

At the *international* level, DOD, in coordination with DOS, works with international partners and allies to ensure defense and defense-related international networks remain operational and secure; coordinates response activities with the armed forces of international partners and allies; and, in close cooperation with DHS, coordinates with the international Computer Security Incident Response Teams (CSIRTs) to synchronize response activities.

Short-Term Recovery

At the *national* level, DOD is responsible for coordinating recovery across the.mil network.

Appendix D: Department of State Roles and Responsibilities

Preparedness

The Department of State facilitates international preparedness, protection, and mitigation efforts related to communications and information technology (IT) infrastructure protection.

Cyber Incident Response

The Department of State leads diplomatic efforts related to Significant Cyber Incidents and reaches out to diplomatic personnel to support the U.S. Government's response to Significant Cyber Incidents. The Department of State serves as a liaison for foreign companies and countries that do not have a U.S. presence in the critical infrastructure and key resources (CIKR) community and that wish or need to engage in incident response activities. The Department of State also serves as a liaison for U.S. citizens affected by Significant Cyber Incidents abroad.

The Department of State facilitates communications with foreign governments to respond to significant communications and IT system disruptions and related incidents. As needed, the Department of State works with the Cyber Unified Coordination Group (UCG) to effect bilateral and multilateral efforts to respond to a cyber-related event.

[This page intentionally left blank.]

Appendix E: Intelligence Community Roles and Responsibilities

Preparedness

At the *national* level, the Intelligence Community (IC), in collaboration with the Department of Defense (DOD) and pursuant to applicable law and policy, provides attack sensing and warning capabilities to characterize the cyber threat and attribution of attacks and to forestall future incidents. The IC coordinates intelligence activities and assists in informing preparedness activities by identifying potential vulnerabilities.

At the *Federal* level, the IC establishes and maintains shared situational awareness across IC networks and shares information with the Department of Homeland Security (DHS) and other partners as appropriate to inform national-level situational awareness. The IC also coordinates preparedness activities, exercises, and lessons learned for stakeholders in the ic.gov space. DHS, DOD, and the Department of Justice (DOJ) work closely with other elements of the IC to share relevant intelligence on cyber threats and vulnerabilities with the private sector and especially the critical infrastructure and key resources (CIKR) community.

At the *international* level, members of the IC work with other departments and agencies and international partners to characterize the cyber threat and attribution of attacks.

Cyber Incident Response

At the *national* level, the IC, upon request, provides representation and leadership support to the Assistant Secretary for the Office of Cybersecurity and Communications (CS&C) in the form of a Cyber Unified Coordination Group (UCG) Senior Official. This representative works with the Assistant Secretary for CS&C to establish and execute unified or joint priorities and overarching objectives for incident response and recovery.

In general, IC entities provide intelligence support and assistance to national response efforts in close coordination with the National Cybersecurity and Communications Integration Center (NCCIC) under all applicable law and policy.

At the *Federal* level, the IC manages incident response efforts across IC networks in close coordination with the NCCIC.

Within the *private sector CIKR* community, the IC works with DHS and other response partners to share appropriate classified intelligence with cleared CIKR sector partners, including Information Sharing and Analysis Centers (ISACs), to allow the provision of sector impact assessments and response coordination. Whenever possible, such intelligence and information should be classified at the lowest level possible.

At the *international* level, the IC utilizes its authorities, resources, and expertise, including the existing Warning Community and Critical Information reporting system, to provide foreign threat-based analysis to all properly cleared, relevant partners with a valid "need to know" and to assist in response efforts. The IC works in close coordination with the NCCIC.

[This page intentionally left blank.]

Appendix F: Department of Justice and Federal Bureau of Investigation Roles and Responsibilities

Preparedness

At the *national* level, the Department of Justice (DOJ), often working through the Federal Bureau of Investigation (FBI), maintains and shares situational awareness about law enforcement activities related to cybersecurity, cyber incidents, and vulnerabilities with the Department of Homeland Security (DHS) and other appropriate law enforcement and cyber incident response partners to inform the national common operational picture. The FBI coordinates InfraGard efforts and ensures situational awareness derived from this effort is integrated into the national common operational picture.

At the *Federal* level, DOJ, including the FBI and law enforcement activities coordinated through the National Cyber Joint Investigative Task Force (NCIJTF), shares domestic investigative information and other information relevant to Federal analysis of threats against cyber infrastructure with DHS and other partners as appropriate, pursuant to established agreements and consistent with law. DOJ provides legal guidance on issues that require resolution during efforts to respond to and recover from a cyber incident. The NCIJTF coordinates cyber-related domestic law enforcement, counterterrorism, and counterintelligence threat investigations.

At the *State and Local* levels, DOJ, including the FBI and the NCIJTF, coordinates with State, Local, Tribal, and Territorial law enforcement to investigate and prosecute cybercrime, cyberterrorism, and counterintelligence matters and share information from these efforts to inform national situational awareness according to the information sharing structures and relationships established in each State.

Within the *private sector critical infrastructure and key resources (CIKR)* community, the FBI coordinates InfraGard efforts and ensures national situational awareness is integrated into InfraGard partners' situational awareness picture. The FBI also works with the private sector in regard to the investigation and prosecution of cybercrime.[45]

At the *international* level, DOJ and FBI, in coordination with other departments and agencies, including the Department of State (DOS), work with other international law enforcement partners to prepare for incidents and maintains situational awareness about foreign cyber threats.

Cyber Incident Response

At the *national* level, DOJ and the FBI provide representation and leadership support to the Assistant Secretary for the Office of Cybersecurity and Communications (CS&C) in the form of a Cyber Unified Coordination Group (UCG) Senior Official. This representative works with the Assistant Secretary for CS&C to establish and execute unified and joint priorities and overarching objectives for incident response and recovery.

In addition, the FBI leads the NCIJTF as a multiagency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, including

[45] InfraGard is a partnership among the Federal Bureau of Investigation (FBI), other governmental entities, and the private sector.

with the National Cybersecurity and Communications Integration Center (NCCIC) as appropriate.

At the *Federal* level, the FBI, through the NCIJTF, coordinates Federal domestic cyber-related counterintelligence, counterterrorism, and criminal law enforcement investigative activities.[46] NCIJTF members take coordinated actions to deter or otherwise prevent cyber attack as authorized by applicable law and policy.[47]

At the *State and Local* levels, DOJ and the FBI support State, Local, Tribal, and Territorial law enforcement investigations of cyber incidents and facilitate information sharing between State, Local, Tribal, and Territorial law enforcement and the national response effort.

Within the *private sector CIKR* community, the FBI coordinates InfraGard efforts and ensures InfraGard is fully integrated into the national response effort.

At the *international* level, DOJ leads the coordination of criminal investigation and prosecution with international law enforcement partners during an incident.

Short-Term Recovery

Working in close coordination with the NCCIC and other law enforcement agencies, DOJ, the FBI, and the other members of the NCIJTF investigate and prosecute cybercrime. In coordination with other law enforcement organizations and the Intelligence Community (IC), the FBI and members of the NCIJTF use their authorities to attribute the source of a cyber attack.

The Attorney General has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States or directed at United States citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States. In cooperation with other Federal departments and agencies engaged in activities to protect national security, the FBI coordinates the activities of law enforcement community members to detect, prevent, pre-empt, and disrupt terrorist attacks against the United States.

DOJ and the FBI coordinate with DHS to provide domestic investigative information relevant to DHS analysis of the continued vulnerability of the cyber infrastructure.

[46] FBI coordinates investigative activities without directing the operational or investigative operations of participating agencies.

[47] FBI leads the National Cyber Joint Investigative Task Force (NCIJTF) as an alliance of peers with complementary missions and coordinates investigations based on complimentary authorities.

Appendix G: All Federal Department and Agency Roles and Responsibilities

Preparedness

Federal departments and agencies are responsible for maintaining an available and cleared security capability to send, receive, and act on alerts at all levels of classification on a 24x7 basis and for ensuring all relevant department and agency cyber information is promptly transmitted to the Department of Homeland Security (DHS) to maintain the common operational picture. All agencies provide cyber-related expertise in support of the National Cyber Incident Response Plan (NCIRP) and cyber incident response as appropriate and consistent with their own responsibilities for protecting our national security, and pre-identify points of contact within their department or agency to serve as Senior Officials in the Cyber Unified Coordination Group (UCG).

In accordance with their responsibilities under the National Infrastructure Protection Plan (NIPP), Sector Specific Agencies (SSA) facilitate real-time cyber incident notification within their respective sectors and provide mechanisms for reporting this information to the DHS National Cybersecurity and Communications Integration Center (NCCIC). SSAs encourage the development of appropriate voluntary information sharing and analysis mechanisms; facilitate the sharing of real-time incident notification; and manage the overall process for building partnerships and leveraging critical infrastructure and key resources (CIKR) security expertise, relationships, and resources within the sector. SSAs are responsible for working with DHS and their respective Government Coordinating Councils (GCC) and Sector Coordinating Councils (SCC) to implement the NIPP sector partnership model and risk management framework; develop protective programs, resiliency strategies, and related requirements; and provide sector-level CIKR protection guidance in line with the overarching DHS guidance pursuant to Homeland Security Presidential Directive 7 (HSPD-7).

As part of these responsibilities, SSAs coordinate sector-level participation in the NCIRP. Representatives of all sectors may, however, coordinate directly with the NCCIC, provided they communicate such participation to their SSA, especially as required by law, regulation, or prior agreement.

Cyber Incident Response

All departments and agencies are responsible for providing full and prompt cooperation, resources, and support consistent with their responsibilities for protecting national security and CIKR. Departments and agencies ensure that, during an incident, all relevant department and agency cyber information is transmitted to the NCCIC via the U.S. Computer Emergency Readiness Team (US-CERT) per Federal requirement and in order to maintain situational awareness. Departments and agencies work with the NCCIC to coordinate their response during a Significant Cyber Incident. All departments and agencies continue to work within their existing missions to perform operational roles and ensure continuation of services by implementing agency-specific incident response plans.

In addition, departments and agencies provide appropriate cyber-related expertise pertaining to the specific incident in support of the NCIRP as requested by DHS, including providing a Senior Official upon request.

SSAs work to communicate relevant sector-related cyber information to the NCCIC to maintain common situational awareness. SSAs also facilitate the sharing of real-time incident information within the sector. NCCIC and NICC communicate cyber information to each other to inform CIKR coordination efforts. In support of the overall objectives established with the Cyber UCG Incident Management Team (IMT), SSAs will work with the NCCIC to facilitate cyber incident response activities.

Short-Term Recovery

Departments and agencies utilize their existing business resumption plans to resume operations as necessary and continue to work within their existing missions to ensure service continuation or restoration in order to facilitate the performance of operational roles. They continue to cooperate and coordinate with DHS in the domestic incident management role.

Following an incident, SSAs ensure all relevant cyber information received continues to be transmitted to the NCCIC. SSAs help coordinate sector-level participation in incident recovery activities.[48]

[48] This may include referring CIKR owners and operators to the NCCIC and/or agencies with more substantial cyber expertise.

Appendix H: State, Local, Tribal, and Territorial Roles and Responsibilities

Preparedness

Chief Executives of each State, Local, Tribal, or Territorial government are responsible for preparedness activities within their State, Locality, Tribe or Territory. These responsibilities include the following:

At the *national* level, as the Chief Executive of a State, Local, Tribal, or Territorial government, each respective leader is responsible for the government's cybersecurity preparedness, response, and recovery procedures. These responsibilities include identifying key individual cyber incident response point(s) of contact for their respective government and ensuring the National Cybersecurity and Communications Integration Center (NCCIC) has the most updated information for these individuals. In addition, to facilitate Significant Cyber Incident response coordination, each Chief Executive should pre-designate a primary individual to serve as a Senior Official to represent its government during a Significant Cyber Incident. Until amended by each Chief Executive, the NCCIC uses the State Homeland Security Advisor as its primary point of contact.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a key resource for State, Local, Tribal, and Territorial government information sharing; early warnings and alerts; mitigation strategies; training; exercises; and maintenance of overall cyber situational awareness. The Federal Government has designated the MS-ISAC to coordinate closely with the Senior Official(s) identified by the Chief Executive and with the Federal Government before, during, and after a Significant Cyber Incident.

Chief Executives should be prepared to request additional resources from the Federal Government, including under the Stafford Act, in the event of a cyber incident that exceeds their government's capabilities.

Predominantly, Homeland Security Offices and Fusion Centers serve as key hubs for information sharing, including for critical infrastructure and key resources (CIKR), within each State. Homeland Security Offices and Fusion Centers take information gathered at the State, Local, Tribal, and Territorial levels and put it into analytic products for use throughout their jurisdiction and at the Federal level. The National Guard is also in a unique position to assist in information sharing, situation awareness, secure communications, and incident response. On a State-by-State basis, Homeland Security Offices, Fusion Centers, and National Guard forces may also play an active role in information sharing for cyber incidents, including the physical effects of cyber incidents. This includes reporting the incident to Federal partners as outlined in the National Cyber Incident Response Plan (NCIRP).

The MS-ISAC can serve as a key resource for Homeland Security Offices and Fusion Centers to report information on cyber incidents to the Federal government. It is important that within each State, Locality Tribe and Territory the cyber reporting mechanisms are clear and understood by all parties to alleviate any reporting issues during a Significant Cyber Incident. This will ensure there is coordination not only with the Federal Government but also that cyber incident reporting provides a common situational awareness at all levels of government versus the potential for fragmented, incomplete, or stove-piped data reporting. The MS-ISAC, in coordination with

State, Local, Tribal, and Territorial governments and the NCCIC, is responsible for tracking and updating State cyber reporting mechanisms.

At the *Federal* level, States provide advice, support, and assistance to Federal departments and agencies on preparedness and response activities related to State, Local, Tribe, and Territory priorities.

At the *State and Local* levels, Chief Executives, Homeland Security Advisors (HSAs), Chief Information Officers (CIOs), and Chief Information Security Officers (CISOs) encourage preparedness activities through participation in cyber exercises; participation in Federal, State, and private sector training activities; and communication between and among States to coordinate situational awareness activities.

The MS-ISAC promotes awareness of the interdependencies between cyber and physical critical infrastructure, as well as between and among the different sectors. It also coordinates training and bi-directional awareness activities.

Cyber Incident Response

At the *national* level, State, Local, Tribal, and Territorial governments, upon request, provide representation and leadership support to the Assistant Secretary for the Office of Cybersecurity and Communications (CS&C) in the form of a Cyber Unified Coordination Group (UCG) Senior Official. To establish and execute unified and joint priorities and overarching objectives for incident response and recovery. To facilitate national incident response coordination, each Chief Executive should make its Senior Official available to represent his or her government during a Significant Cyber Incident and should ensure the government's reporting mechanisms are clear and understood by the NCCIC.

At the *Federal* level, States, Localities, Tribes, and Territories provide advice, support, and assistance to Federal departments and agencies on response activities related to State, Local, Tribe, and Territory priorities and systems.

At the *State and Local* levels, Governors and their representatives work within the State, Localities, Tribes, and Territories to ensure execution of response activities. This effort includes coordinating with the NCCIC, the MS-ISAC, and the State's designated Senior Official to ensure close coordination of priority response efforts.

Short-Term Recovery

States may request assistance from the Federal Government under the Stafford Act as necessary. The State is responsible for the recovery of State systems and may request technical assistance from the NCCIC or other incident partner, as required.

Appendix I: Private Sector Critical Infrastructure and Key Resources Community Roles and Responsibilities

Preparedness

At the *national* level, many in the critical infrastructure and key resources (CIKR) community participate in Information Sharing and Analysis Centers (ISACs), which advance physical and cyber CIKR protection and preparedness by establishing and maintaining collaborative frameworks for operational interaction between and among members and external partners. ISACs, as identified by the sector's Sector Coordinating Council (SCC), typically serve as the tactical and operational arms for sector information sharing efforts. Sector Specific Agencies (SSA) serve as a coordination mechanism for sectors not represented by an ISAC or that choose not to coordinate directly with the National Cybersecurity and Communications Integration Center (NCCIC). Many of these organizations are described in Appendix N.

At the *Federal* level, the CIKR community provides advice, support, and assistance to Federal departments and agencies on preparedness and response activities. The CIKR community works with its SSAs to improve preparedness and manage risk.

At the *State and Local* levels, the CIKR community provides advice, support, and assistance to State, Local, Tribal, and Territorial partners on preparedness and response activities.

Within the *private sector CIKR* community, private sector CIKR partners work to improve industry-wide situational awareness and expand strategic analytical capabilities. This work facilitates public and private sector security partner collaboration to identify potential incidents and ensure informal relationships can be leveraged during a cyber incident. Many CIKR sectors utilize ISACs and other sector-designated operational entities to coordinate analysis and conduct information sharing activities. The NCCIC will work closely with these organizations to help facilitate the flow and analysis of information.

At the *international* level, as appropriate, organizations maintain key international relationships and communications mechanisms to prepare for incidents and maintain situational awareness of potential international threats. They develop and maintain awareness of key international supply chain dependencies; establish mechanisms to quickly respond to vulnerabilities introduced by foreign dependencies; and develop and maintain capabilities to respond to and recover from incidents outside of the United States that may affect their mission-critical functions or critical U.S. networks.

Cyber Incident Response

As part of their regular communications, private sector organizations should work with each other to establish response priorities and communicate about incident activities. This effort should include leveraging existing mechanisms and processes for communicating with other sectors and collaborating with law enforcement to rapidly identify and mitigate criminal activities that could potentially harm the sector's infrastructure.

At the *national* level, private sector organizations, especially those in the CIKR community, will be asked to provide representation and leadership support to the Assistant Secretary for the Office of Cybersecurity and Communications (CS&C) to establish and execute unified and joint priorities and overarching objectives for incident response and recovery. They should be empowered by their company or organization to be able to make senior-level decisions regarding

the voluntary commitment of resources and personnel and to make decisions about the operations of their networks and/or communications assets.

At the *State and Local* levels, and as part of their existing relationships with State, Local, Tribal, and Territorial governments, the private sector may provide support and services to assist State, Local, Tribal, and Territorial governments.

At the *international* level, and organization by organization, the private sector should work with international components and business partners and through other international relationships to coordinate and synchronize response activities affecting its networks and systems. When assistance with foreign governments is needed, companies may ask the State Department to assist with international coordination.

Short-Term Recovery

Individual companies and sectors are responsible for the short-term recovery of their systems but may request technical assistance as needed from Federal partners at the NCCIC or through pre-established relationships.

Appendix J: Executive Office of the President

Preparedness

At the *national* level, the White House coordinates interagency policy formulation and the resolution of policy-related challenges. The President's Cybersecurity Coordinator, working with the Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC), determines the most efficient and effective method of developing and maintaining situational awareness and incident response capabilities. Depending on the scenario, a variety of interagency policy groups might help coordinate.

At the *Federal* level, the National Communications System (NCS) assists the President, National Security Council (NSC), Homeland Security Council, Director of the Office of Science and Technology Policy (OSTP), and Director of the Office of Management and Budget (OMB) in the exercise of the communications functions and responsibilities set forth in Section 2 of Executive Order 12472, as amended, as well as in the coordination of planning for and providing National Security and Emergency Preparedness (NS/EP) communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. The NCS also provides support to the policy coordination role of the Director of OSTP.

OMB oversees the implementation of government-wide policies, principles, standards, and guidelines for Federal computer security programs and can issue directives for departments and agencies to protect networks. OMB provides budgetary guidelines and coordinates the activities of the Federal Chief Information Officer (CIO) Council. The White House is responsible for giving the Department of Defense (DOD) the authority to respond to a cyber attack.

At the *international* level, the White House provides clarity on the U.S. Government's policy toward network attacks carried out overseas that have major domestic implications for the United States. In coordination with the Department of State (DOS), Department of Homeland Security (DHS), and other departments and agencies, the White House engages with international partners to improve security and plan for international cyber incidents.

Cyber Incident Response

At the *national* level, the White House is responsible for coordinating interagency policy formulation and will resolve policy-related challenges that arise during implementation of the National Cyber Incident Response Plan (NCIRP). The President's Cybersecurity Coordinator, working with the ICI-IPC, will determine and implement the most efficient and effective method of developing and maintaining interagency situational awareness for policy-related activities. Depending on the effects of the incident, different White House interagency policy groups might be involved in policy coordination activities. The National Security Staff (NSS) provides policy direction for execution of the Presidential authority under Section 706 of the Communications Act of 1934, as amended, with OSTP directing exercise of that authority if the President determines that certain preconditions have been satisfied.

The NCS assists the President, NSC, Homeland Security Council, Director of OSTP, and Director of OMB in coordinating the plan for and provision of NS/EP communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. NCS also leads and manages the joint industry-government National Coordinating Center (NCC), which assists in the initiation, coordination, restoration, and

reconstitution of NS/EP communications services or facilities under all conditions of crisis or emergency. The Director of OSTP chairs the Joint Telecommunications Resource Board (JTRB). The JTRB assists the Director of OSTP in providing information, advice, guidance, and assistance, as appropriate, to the President and to those Federal departments and agencies with responsibilities for the provision, management, or allocation of telecommunications resources during those crises or emergencies in which the exercise of the President's war power functions is not required or permitted by law.

The Cybersecurity Coordinator serves as the White House focal point for cyber incident response (a similar role to the Senior Officials who help the White House monitor terrorist attacks or natural disasters).

OMB oversees the implementation of government-wide policies, principles, standards, and guidelines for Federal Government computer security programs and can issue directives for departments and agencies to take in order to protect networks. OMB also provides budgetary guidelines and coordinates activities of the Federal CIO Council.

At the *international* level, the White House can provide clarity on the U.S. Government's policy toward network attacks carried out overseas that have major domestic implications for the United States. In coordination with departments and agencies, the White House engages with international partners to improve security and plan for international cyber incidents.

Appendix K: The National Cyber Risk Alert Level System

Introduction

The National Cyber Risk Alert Level (NCRAL) system operates as a national-level alert and warning system that conveys the current level of cyber risk[49] to critical infrastructure and key resources (CIKR) critical functions. The system utilizes the common operational picture from the National Cybersecurity and Communications Integration Center (NCCIC) and works with NCCIC partners to examine risk to cybersecurity systems across CIKR sectors and across the Nation. When risk to critical systems is determined, it will be communicated through four alert levels (Guarded, Elevated, Substantial, Severe) and will be accompanied by additional, more detailed information as described in the Alert Levels section of this Appendix.

Scope

The NCRAL system focuses primarily on—

- Confidentiality, integrity, or availability in the cyber domain
- Observed or potential consequences of threats, vulnerabilities, and events, especially as related to—
  - National security
  - Public health and public safety
  - National economy, including any of the individual sectors that may affect the national economy
  - Public confidence
  - Any combination of these categories at the national, regional, or sector level.[50]

The NCRAL system is based on an assessment of—

- Actual cyber incidents
- Threat, vulnerability, and consequence information provided by a variety of sources, including Federal, State, Local, Tribal, Territorial and private sector partners
- Current levels of other private and public cyber alert level systems.

Determining National Cyber Risk/Setting the Alert Level

The core elements used to determine cyber risk and set the alert level are—

- The common operational picture provided by the NCCIC and NCCIC partners
- Analysis and evaluation of relevant information
- Analysis of a cyber incident or series of incidents
- Estimation of whether significant cyber assets or enabling systems have been, or may be, exploited successfully
- Determination of national-level consequences
- Working with NCCIC partners to determine whether to raise, lower, or retain the current NCRAL.

[49] The NCRAL system examines the following risk factors: threats (activities and event indicators of a potential cyber incident), vulnerabilities (potential threat exploitation paths), and consequences (abnormal performance or degradation of critical functions).

[50] The alert system may also include such factors as degradation to mission and psychological effects as outlined in the NIPP.

As depicted in Figure 10, the NCRAL system utilizes NCCIC processes to bring together cybersecurity information sources and risk assessment information sources to determine the overall NCRAL:

- **Cybersecurity Information Sources:** The NCCIC brings together relevant information to present a consolidated operational picture that may affect the cybersecurity environment at a national level.
- **Risk Assessment Information Sources:** The Department of Homeland Security (DHS) risk assessment process looks at the cybersecurity information provided to the NCCIC and applies a variety of factors, such as CIKR sector dependency information, CIKR sector critical functions, and national-level risk and consequence information.
- **The NCRAL Condition:** As cyber information is brought together and analyzed at the NCCIC, cyber consequences, sector dependency, and critical function information are analyzed in a national-level context. Factors such as threats, threat actors, vulnerabilities, and potential or observed consequences provide the basis for determining the current level of cyber risk to national-level critical functions. The NCRAL is determined based on the analysis of these information sources (see Figure 10).

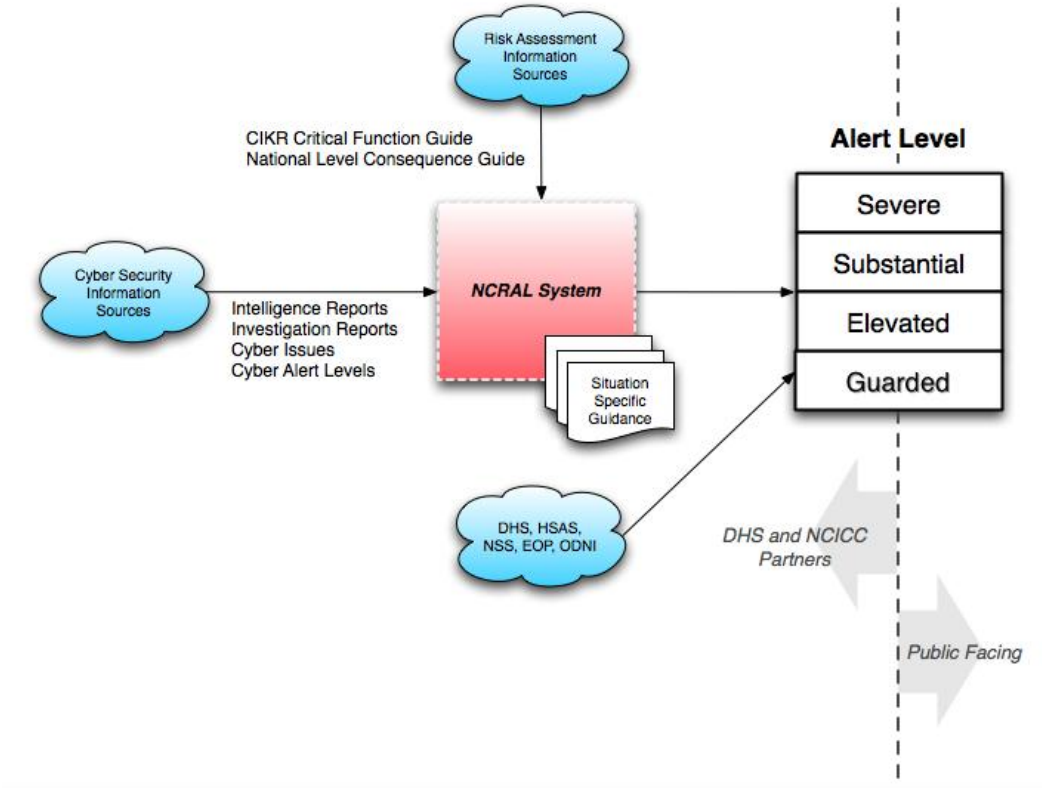


Figure 10: NCRAL System High-Level Overview

Cybersecurity Information Sources

The NCCIC common operational picture brings together relevant information to inform national-level decision making, including preparedness and response activities and the operational posture of any response efforts. As part of the common operational picture, the NCCIC receives information on threats, vulnerabilities, and potential consequences from cybersecurity information sources and risk assessment information sources.

Cybersecurity information sources, as illustrated in Figure 11, include information from intelligence reports, criminal investigation reports, cyber alert levels from private sector and cybersecurity vendors, and reports and discoveries of specific cyber issues from miscellaneous sources. This information is used to determine an overarching understanding of which cyber assets may be at risk and is then analyzed in the context of risk assessment information.

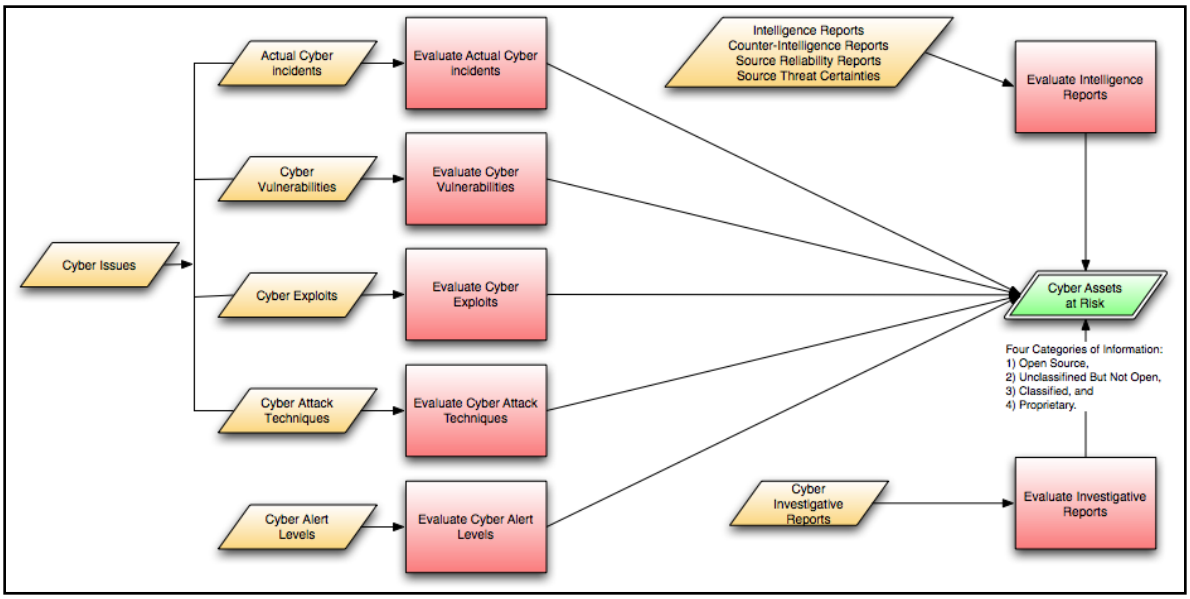


Figure 11: Cybersecurity Information Sources

Risk Assessment Information Sources

The DHS risk assessment process leverages specific CIKR sector dependency information sources, including CIKR sector critical functions and national-level risk and consequence information. These inputs come from sector leads and NCCIC partners in accordance with information sharing agreements. This risk assessment process has two primary goals:

1. Provide guidance on how the potential exploitation of a significant cyber asset could degrade one or more critical functions performed by a CIKR organization (this is referenced in Figure 12 as "CIKR Critical Function Guide based on Mapping").
2. Provide guidelines on how the degradation of each critical function could result in a national-level consequence and the expected severity of that result (this is referenced in Figure 12 as "National-Level Consequence Guide based on Mapping").

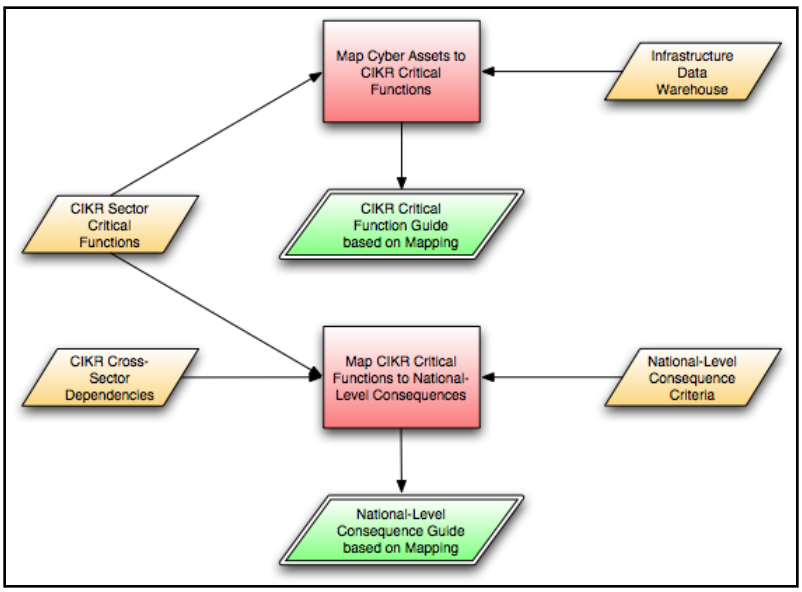


Figure 12: Cyber Consequence Assessment

These inputs are used to determine possible national-level consequences based on overall national risk. This information is combined with several other information points to determine a comprehensive risk picture. These information points include—

- **Cyber Threat Characteristics:** Contained in the information technology (IT) Sector Baseline Risk Assessment; includes sophistication, skill level, tools, money, time, access (physical or logical), and limitations
- **Cyber Vulnerability Characteristics:** Also contained in the IT Sector Baseline Risk Assessment; includes applicability, extent of exposure, availability, and simplicity
- **Cyber Assets at Risk:** Exploited, targeted, and vulnerable significant cyber assets, as well as significant cyber threat actors, as related to a specific or potential adverse cyber effect driving toward a cyber exploitation
- **National-Level Consequence at Risk:** The set of national-level consequences presently at risk and the severity of each associated consequence certainty
- **CIKR Response Capability:** The capability of the CIKR response community to respond to and mitigate national-level consequences adequately and in a timely manner
- **NCRAL Guide:** Provides the criteria to determine the alert level; if the CIKR response capability is adequate for each of the national-level consequences at risk, then the NCRAL remains at or moves to Level 4 (Guarded).

The overall process is depicted in Figure 13.

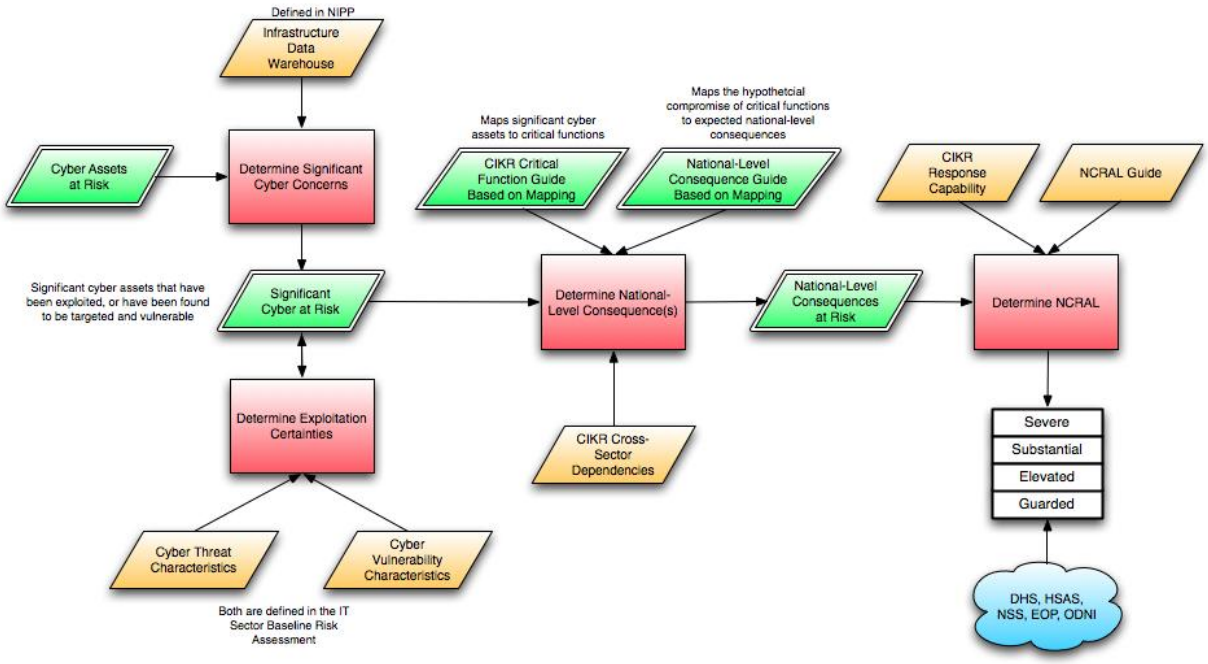


Figure 13: Overall NCRAL Process

These inputs are taken together and provide a mechanism to determine overall cyber risk to critical assets and systems.

Setting the Alert Level

The Assistant Secretary for the Office of Cybersecurity and Communications (CS&C) determines the alert level of the NCRAL system in coordination with recommendations from NCCIC partners. When setting the NCRAL at Levels 2 or 1, the Assistant Secretary takes into special consideration whether the conditions outlined in Homeland Security Presidential Directive 5 (HSPD-5) have been triggered. These include—

- A Federal department or agency acting under its own authority has requested the assistance of the Secretary
- The resources of State Local, Tribal, and Territorial authorities are overwhelmed, and Federal assistance has been requested by the appropriate State, Local, Tribal, and Territorial authorities
- More than one Federal department or agency has become substantially involved in responding to the incident
- The Secretary has been directed to assume responsibility for managing the incident by the President.

The alert level of the NCRAL system is set based on the NCRAL Guide (see Table 1).

Consequences:	NCRAL Alert Level Guide			Set the NCRAL to:
	Have Been Verified/Observed	Are Suspected/Indicated	Are Potential/Not Indicated	
Severity of consequences are or would be:	Minimal	Minimal	Minimal	4—Guarded
			Moderate	
			Significant	
			Severe	
		Moderate	Moderate	
			Significant	
			Severe	
		Significant	Significant	3—Elevated
			Severe	
		Severe	Severe	
	Moderate	Moderate	Moderate	
			Significant	
			Severe	
		Significant	Significant	
			Severe	
		Severe	Severe	2—Substantial
	Significant	Significant	Significant	
			Severe	
		Severe	Severe	1—Severe
	Severe	Severe	Severe	

Table 1: National Cyber Risk Alert Levels

The alert level is communicated to the public with appropriate guidance from the NCCIC in coordination with established external affairs procedures. It can also be disseminated to various government agencies and appropriate CIKR sectors with appropriate, specific, and actionable information. The cycle of input, analysis, level determination, and dissemination is repeated on an ongoing basis.

NCRAL Alert Levels

The NCRAL levels are designed to inform preparedness, decision making, information sharing, and cyber incident management activities (see Table 2). Specific alert levels will be associated with actions and timeframes whenever possible, in accordance with the NCCIC Concept of Operations (CONOPS). The Assistant Secretary for CS&C will examine the alert level consistently in order to return to the baseline level of Level 4 or "Guarded."

Because the impact or criticality of a particular cyber threat, vulnerability, or consequence varies dramatically across the Government and CIKR sectors and organizations, the NCRAL system retains the flexibility to raise or lower the alert level on a sector-by-sector basis in coordination with sector stakeholders. It lowers when the added capabilities offered by higher alert levels are no longer needed. Although the public affairs posture may change between each alert level, the NCCIC retains the capacity to coordinate the public affairs response at any NCRAL level in accordance with the NCCIC Public Affairs coordination plan.

Level	Label	Description of Risk	Level of Response
1	**Severe**	Highly disruptive levels of consequences are occurring or imminent	Response functions are overwhelmed, and top-level national executive authorities and engagements are essential. Exercise of mutual aid agreements and Federal/non-Federal assistance is essential.
2	**Substantial**	Observed or imminent degradation of critical functions with a moderate to significant level of consequences, possibly coupled with indicators of higher levels of consequences impending	Surged posture becomes indefinitely necessary, rather than only temporarily. The DHS Secretary is engaged, and appropriate designation of authorities and activation of Federal capabilities such as the Cyber UCG take place. Other similar non-Federal incident response mechanisms are engaged.
3	**Elevated**	Early indications of, or the potential for but no indicators of, moderate to severe levels of consequences	Upward shift in precautionary measures occurs. Responding entities are capable of managing incidents/events within the parameters of normal, or slightly enhanced, operational posture.
4	**Guarded**	Baseline of risk acceptance	Baseline operations, regular information sharing, exercise of processes and procedures, reporting, and mitigation strategy continue without undue disruption or resource allocation.

Table 2: National Cyber Risk Alert Levels

Along with specific information about the threat, each level can inform and guide appropriate responses. At Levels 1 (Severe) and 2 (Substantial), a Significant Cyber Incident has occurred, and the NCCIC and its partners respond accordingly.

Level 4 (Guarded)

Level 4 is the baseline of normal risk; it can represent known nefarious activity with sufficient public mitigation strategies. This activity includes daily intrusions and probes from sources around the world that induce minimal consequences but no indications that would raise concerns for higher level consequences. An appropriate response would be to continue baseline operations, regular information sharing, exercise of processes and procedures, reporting, and mitigation strategies without undue disruption or resource allocation. This baseline level will evolve over time with changes in the threat, vulnerability, and consequence landscape.

When the NCCIC receives information on Level 4 activities, the NCCIC Senior Watch Officer (SWO) works with the originator(s) of the information to ensure the information or summary receives the widest possible dissemination at the appropriate level of detail.

If the NCCIC receives information that may indicate the activity is more widespread than initially indicated, the NCCIC may issue a broad request for information.

Characteristics and criteria at Level 4 include—

- The threat affects only non-mission-critical system(s)[51] (e.g., individual workstations)
- The ability to detect, deter, respond, and resolve the issue(s) is exercised as part of normal daily operations and capabilities
- Only steady-state levels of communication or reporting are required
- Information sharing products are able to be updated and distributed per existing procedures
- Events, impacts, and new information are catalogued per normal procedures
- Direct outreach to other potential targeted or affected groups may be conducted per existing procedures
- Any preparedness, mitigation, and response measures should be able to be maintained indefinitely as a part of normal operations.

Level 3 (Elevated)

Level 3 reflects risk factors with moderate or greater consequence potential, requiring increased precaution and vigilance. Some activities taken to mitigate the risk may impose some disruption of normal functions and may require temporary surge activities. At Level 3, most responding entities are capable of managing incidents and events within the parameters of normal, or slightly enhanced, operational posture or through coordination with NCCIC partners.

When the NCCIC receives information on activities that rise to Level 3, the NCCIC SWO notifies and provides information to the NCCIC Director, who will inform the Assistant Secretary for CS&C and the Cyber UCG Staff. If the Assistant Secretary for CS&C has delegated the alert level designation authority to the NCCIC Director, the Director may set the level at Level 3.

At Level 3, the NCCIC Director works with the Cyber UCG Staff to evaluate the information and work through each Cyber UCG Staff department, agency, or organization to ensure Cyber UCG organizations are actively reporting information of a similar nature. The NCCIC SWO works with the originator(s) of the information to ensure the information receives the widest possible dissemination at the appropriate level of detail. The NCCIC Director must report every 24 hours to the Assistant Secretary for CS&C on the recommended level.

Characteristics and criteria at Level 3 include—

- Known or expected intrusion activity is present or reported, in addition to other criteria listed below
- The impact of zero-day exploit discovery or release is unknown
- Evidence exists of a successful intrusion that affects critical systems but does not substantially degrade them

[51] Mission-critical systems will vary by organization providing input into the NCRAL. When assessing mission criticality, each organization is encouraged to develop a standard methodology for determining the importance of systems relative to the achievement of organizational goals and objectives. An example of such a system is DOD's Mission Assurance Categories.

- Intelligence reporting indicates increased activity from "cyber based" adversaries
- The Secretary of Homeland Security activates the DHS Crisis Action Team (CAT)
- The ability to detect, deter, respond, and resolve the issue(s) is exercised as part of normal daily operations and capabilities or temporarily surged operations
- Preparedness, mitigation, and response measures should be able to be maintained indefinitely as a part of normal or slightly surged operations
- Some special, event-specific communication or reporting is required
- Direct outreach and coordination with affected entities is required above that taken at Level 4
- Events, impacts, and new information can still be catalogued per normal procedures
- Direct outreach to other potential targeted or affected groups may be conducted per existing procedures
- Vulnerability assessment and corrective action is necessary.

Level 2 (Substantial)

Level 2 reflects observed or imminent degradation of critical national-level functions with a moderate to significant level of consequences, possibly coupled with indicators of higher levels of consequences impending. Normal functions are significantly disrupted, and mitigation measures will likely entail significant disruptions and resource allocation. At Level 2, some or all critical response functions become strained or overwhelmed, and a surged posture becomes indefinitely necessary, rather than only temporarily. The DHS Secretary is engaged, and appropriate designation of authorities and activation of Federal capabilities such as the Cyber UCG take place. Other similar non-Federal incident response mechanisms are engaged. Exercise of mutual aid agreements and Federal assistance may be warranted.

At the NCCIC, a threat, vulnerability, or potential consequence that initially began as a Level 3 threat may be recognized as a larger threat than initially reported. The Assistant Secretary for CS&C, in consultation with the NCCIC Director and the Cyber UCG Staff, determines whether the threat warrants setting the NCRAL system at Level 2. In doing so, the Assistant Secretary for CS&C considers the full ramifications of setting the System at Level 2, including any effects it may have on public confidence in other public or private sector entities.

When the Assistant Secretary for CS&C sets the cyber alert level at Level 2, the NCCIC Director continues to coordinate cyber incident management and response activities, and the Assistant Secretary for CS&C begins reporting on the incident to the Secretary in coordination with the National Operations Center (NOC). The Assistant Secretary for CS&C notifies the Secretary of Homeland Security, NPPD leadership, and the White House Cyber Coordinator. The Assistant Secretary for CS&C notifies the Cyber UCG Staff and Senior Officials. The Manager of NCS provides situational awareness to the Office of Science and Technology Policy (OSTP) and to the Under Secretary of the National Protection and Programs Directorate (NPPD). The NCCIC Director notifies the NOC and the National Infrastructure Coordinating Center (NICC) and issues a notification to NCCIC partners and other audiences as appropriate. At Level 2, organizations that have responded on their own should notify the NCCIC and coordinate further actions as part of the national response effort.

The Cyber UCG Staff recommends Senior Officials to be brought into the Cyber UCG Incident Management Team (IMT) to the Assistant Secretary for CS&C. These recommendations are based on the assets affected by the incident, severity and scope of the incident, capabilities, and legal authorities. The Assistant Secretary for CS&C selects the Cyber UCG IMT, serves as cyber incident manager at the NCCIC, and coordinates Cyber UCG IMT activities. Based on the

incident, the Cyber UCG IMT may choose to solicit advice or include others based on further analysis (additional parties may be able to help resolve the incident or help manage cyber risk). The Cyber UCG IMT, as an interagency body, determines the incident action plan to be carried out by each agency and organization and sets strategies, goals, and intended outcomes of the response effort.

Characteristics and criteria at Level 2 include—

- Major disruption in critical functions is imminent or in progress
- Impacts on .gov or .mil infrastructure, in addition to other non-Federal systems, are occurring
- Intrusion into or disruption of classified networks is occurring
- An incident involving a top-level or second-level domain name server is occurring
- A targeted intrusion or exploit of publicly significant systems, such as the White House network, is occurring
- The impact of zero-day exploit discovery or release is unknown
- Evidence exists of a successful, focused attack(s) that affects or may affect critical functions
- Unauthorized root-level access across Federal agency boundaries is occurring
- Preparedness, mitigation, or response measures are overwhelmed or only possible at a significant and indefinitely surged posture
- National-level National Cyber Incident Response Plan (NCIRP) procedures and authorities are fully engaged
- Regular increased event-specific communication or reporting is required
- Regular increased information sharing activities are required
- Continued direct outreach and coordination with affected entities is required
- Continued direct outreach to other potential targeted or affected groups may be conducted per existing procedures
- Exercise of mutual aid agreements or Federal assistance to non-Federal entities is still warranted
- Aggressive and coordinated collective response, recovery, and mitigation activities are still required
- Public affairs coordination is essential.

Level 1 (Severe)

Level 1 reflects that severe levels of consequences are occurring or imminent. Highly disruptive mitigation measures are likely required to alleviate the consequences and address the threat. Normal functions may be suspended or deferred, cyber response functions are overwhelmed, and top-level national executive authorities and engagement are essential. Exercise of mutual aid agreements and Federal or non-Federal assistance are essential.

If a Level 1 event occurs without a Level 2 alert, the Assistant Secretary for CS&C sets the cyber alert level at Level 1, the NCCIC Director will continue to coordinate cyber incident management and response activities, and the Assistant Secretary for CS&C begins reporting to the Secretary in coordination with the NOC. The Assistant Secretary for CS&C notifies the NOC, NPPD leadership, and White House Cyber Coordinator. The Assistant Secretary for CS&C notifies the Cyber UCG Staff and Senior Officials. The Manager of NCS provides situational awareness to OSTP and NPPD leadership. The NCCIC Director notifies the NOC and issues a notification to NCCIC partners and other audiences as appropriate. As at Level 2, at Level 1, organizations that may have responded on their own should notify the NCCIC and coordinate further actions as part of the national response effort.

The Assistant Secretary for CS&C selects the Senior Officials to be brought into the Cyber UCG IMT based on capabilities and legal authorities. The Assistant Secretary for CS&C serves as cyber incident manager at the NCCIC and coordinates Cyber UCG IMT activities. The Cyber UCG IMT may choose to solicit advice or include others based on further analysis (additional parties may be able to help resolve the incident or help manage cyber risk). The Cyber UCG IMT will determine possible courses of action for each agency to carry out and will develop a response plan for the cyber incident.

Characteristics and criteria at Level 1 include—

- Intrusion into or disruption of classified networks is occurring
- Major disruption in critical functions is occurring over a large part of the cyber infrastructure
- Major disruption to .gov, .mil, .com, or other top-level domains is occurring
- Major cyber-related disruption of critical functions or disruption/destruction of assets is occurring over a large part of other CIKR
- Known significant impact of zero-day exploit discovery or release exists
- Intelligence and other reporting confirms malicious activity from "cyber based" adversaries
- Intelligence and other reporting confirms relationship between cyber incident and hostile military action against the United States or U.S. allies, including acts of war
- Preparedness, mitigation, or response measures are overwhelmed
- White House and senior non-Federal executive action is required
- National-level NCIRP procedures and authorities are fully engaged
- Full and ongoing activation of Cyber UCG is necessary
- Regular special, event-specific communication or reporting is required
- Regular special information sharing activities are required
- Exercise of mutual aid agreements or Federal assistance to non-Federal entities is essential
- Non-Federal assistance to Federal entities is essential
- Aggressive and collective response, recovery, and mitigation activities are required.

[This page intentionally left blank.]

Appendix L: Authorities[52]

Key Authorities

- Title II, Homeland Security Act (Title II, Public Law 107-296)
- Homeland Security Presidential Directive (HSPD) 5: *Management of Domestic Incidents*
- HSPD-7: *Critical Infrastructure Identification, Prioritization, and Protection*
- HSPD-8: *National Preparedness*
- National Security Presidential Directive (NSPD) 51/HSPD-20: *National Continuity Policy*
- NSPD-54/HSPD-23: *Cybersecurity Policy*
- Federal Information Security Management Act (FISMA)
- Executive Order 12382: *President's National Security Telecommunications Advisory Committee*
- Executive Order 12472: *Assignment of National Security and Emergency Preparedness Telecommunications Functions*
- Executive Order 12333: *United States Intelligence Activities*
- Section 706, Communications Act of 1934, as amended (47 U.S.C. 606)
- Defense Production Act of 1950, as amended
- National Security Act of 1947, as amended
- National Security Directive 42: *National Policy for the Security of National Security Telecommunications and Information Systems*
- Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458, 118 Stat. 3638)
- Intelligence Authorization Act for Fiscal Year 2004 (Public Act 108-177)
- Title 10 United States Code (U.S.C.) and Title 32 U.S.C.
- Title 18 U.S.C. and Title 50 U.S.C.

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

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

Several industries operate under regulatory structures that require reporting and coordination. These include—

[52] This section does not include key policy documents, including the National Strategy to Secure Cyberspace and the NIPP.

- Many financial services sector companies
- Many chemical sector companies
- Utilities companies
- Regulated communications companies.

Appendix M: Definitions

Common Operational Picture	A continuously updated overview of an incident compiled throughout an incident's lifecycle from data shared between integrated systems for communication, information management, and intelligence and information sharing. The common operational picture allows Incident Managers at all levels to make effective, consistent, and timely decisions. The common operational picture also helps ensure consistency at all levels of incident management across jurisdictions, as well as between various governmental jurisdictions and private sector and nongovernmental entities that are engaged.	National Response Framework (NRF)
Cross-Domain Situational Awareness	The set of timely cross-domain national-level information that will provide situational awareness on the state of U.S. cyber networks and systems to (1) know the availability, integrity, and confidentiality of U.S. cyber networks and systems, (2) understand the current and potential threats to U.S. cyber networks and systems, and (3) ensure that legitimate network operations are not mistaken for malicious activity.	National Cyber Security Center (NCSC) Concept of Operations (CONOPS)
Critical Cyber System/Asset/Function	Is considered to be vital if a physical or cyber incident affecting the confidentiality, integrity, and availability of the system, asset, or function would have significant negative impact on the national security, economic stability, public confidence, health, or safety of the United States.	Multi-State Information Sharing and Analysis Center (MS-ISAC)
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, Regional, Territorial, or Local jurisdiction.	National Infrastructure Protection Plan (NIPP)
Critical Infrastructure Owner and Operator	Those entities responsible for day-to-day operation and investment in a particular asset or system.	NIPP
Critical Infrastructure and Key Resources (CIKR) Partner	Those Federal, State, Local, Tribal, or Territorial governmental entities, public and private sector owners and operators and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share in the responsibility for protecting the Nation's CIKR.	NIPP
Cyber Infrastructure	Includes electronic information and communications systems and services and the information contained therein. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example, computer systems; control systems (e.g., Supervisory Control and Data Acquisition); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.	NIPP
Cyberspace	A global domain consisting of the interdependent network of information technology infrastructures; includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.	White House Cyberspace Policy Review, National Security Presidential Directive (NSPD) 54/Homeland Security Presidential

		Directive (HSPD) 23, and Joint Publication (JP) 1-02
Domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.	National Institute for Standards and Technology (NIST) Interagency Report (IR) 7298
Denial of Service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.	NIST Special Publication (SP) 800-61
Defense Support of Civil Authorities	Department of Defense (DOD) support, including Federal military forces, the Department's career civilian and contractor personnel, and DOD agency and component assets, for domestic emergencies and for designated law enforcement and other activities. DOD provides Defense Support of Civil Authorities when directed to do so by the President or the Secretary of Defense. Defense Support of Civil Authorities can be activated via three primary mechanisms. Federal assistance, including assistance from DOD, can be provided (1) at the direction of the President, (2) at the request of another Federal agency under the Economy Act, or (3) in response to a request from the Department of Homeland Security's Federal Emergency Management Agency under the Stafford Act. The second and third mechanisms require a request for assistance and approval of the Secretary of Defense.	Office of the Assistant Secretary of Defense (OASD) for Homeland Defense
Intrusion	Unauthorized act of bypassing the security mechanisms of a system.	Committee on National Security Systems (CNSS) Information Assurance (IA) Glossary
Information and Communications Technology	An umbrella term that includes information technology and any communication devices or applications, encompassing radio, television, cellular phones, computer and network hardware and software, satellite systems, and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning.	40 United States Code Section 1401
Key Resources	Any publicly or privately controlled resources essential to the minimal operations of the economy and Government.	NRF
Mitigation	Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident. Includes solutions that contain or resolve risks through analysis of threat activity and vulnerability data, which provide timely and accurate responses to prevent attacks, reduce vulnerabilities, and fix systems.	U.S. Computer Emergency Readiness Team (US-CERT) CONOPS, NIPP
National Security and Emergency Preparedness (NS/EP) Communications	Those communications services which are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States.	47 Code of Federal Regulations (CFR) Chapter II, § 201.2(g)
Open Source Information	Open source information is publicly available information, including information with limited distribution or access, including information available by subscription.	
Preparedness	Actions that involve a combination of planning, resources, training,	NRF

	exercising, and organizing to build, sustain, and improve operational capabilities. Preparedness is the process of identifying the personnel, training, and equipment needed for a wide range of potential incidents, and developing jurisdiction-specific plans for delivering capabilities when needed for an incident.	
Prevention	Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.	NRF
Private Sector	Organizations and entities that are not part of any governmental structure. The private sector includes for-profit and not-for-profit organizations, formal and informal structures, commerce, and industry. Please also refer to Critical Infrastructure Owner and Operator.	NRF
Protection	Actions or measures taken to cover or shield from exposure, injury, or destruction. In the context of the National Infrastructure Protection Plan, protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities; building resiliency and redundancy; incorporating hazard resistance into initial facility design; initiating active or passive countermeasures; installing security systems; promoting workforce surety, training, and exercises; and implementing cybersecurity measures, among various others.	NIPP
Recovery	The development, coordination, and execution of service and site restoration plans; the reconstitution of government operations and services; individual, private sector, nongovernmental, and public assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.	NRF
Response	Immediate actions to save lives, protect property and the environment, and meet basic human needs. Response also includes the execution of emergency plans and actions to support short-term recovery.	NRF
Sector-Specific Agency	A Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category.	HSPD-7
Significant Cyber Incident	A Level 2 or Level 1 Incident on the Cyber Risk Alert Level System. A Significant Cyber Incident is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the Nation. A Significant Cyber Incident may destroy, degrade, or disrupt the cyber infrastructure and/or the integrity of the information that supports the	

	private and public sectors. Complications from a Significant Cyber Incident may threaten public health or safety, undermine public confidence, have a debilitating effect on the national economy, or diminish the security posture of the Nation. A Significant Cyber Incident may adversely affect the Nation's ability to project force and may have implications on the Nation's Strategic Deterrence capability. Rapid identification, information exchange, investigation, response, and remediation often can mitigate the damage that a Significant Cyber Incident can cause and aid in rapid recovery and reconstitution after and during an incident.	
Situational Awareness	The knowledge and understanding of the current operational status, risk posture, and threats to the cyber environment gained through instrumentation, reporting, assessments, research, investigation, and analysis, which are used to enable well-informed decisions and timely actions to pre-empt, deter, defend, defeat, or otherwise mitigate against those threats and vulnerabilities.	Comprehensive National Cybersecurity Initiative (CNCI) 5
Shared Situational Awareness	The comprehensive, cross-network domain knowledge resulting from combining and synthesizing relevant, timely, and comprehensive situational awareness information, tailored to the needs of each organization, which enables a transformational improvement in their ability to operate, maintain, and defend their networks or perform their cybersecurity missions.	CNCI-5
Support	A temporary relationship between organizations by which one organization responds to requests or otherwise assists another organization in enhancing its mission effectiveness or efficiency during the conduct of operations. The *supporting organization* provides the assistance, and *the supported organization* receives the assistance. These terms apply to different organizations operating together in a joint environment. The support may involve operational assistance, technical assistance, resources, liaison, information, or other forms of capability enhancement. The *supporting organization* responds directly to requests from the *supported organization*.	
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	NIST SP 800-53, Committee on National Security Systems Instruction (CNSSI) 4009 Adapted
Vulnerability	A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.	NIST SP 800-53, Federal Information Processing Standard (FIPS) 200, CNSSI-4009 Adapted

Appendix N: Organizations

The Executive Office of the President

President Franklin D. Roosevelt created the Executive Office of the President (EOP) in 1939 to provide the President with the support he or she needs to govern effectively. The EOP has responsibility for tasks ranging from communicating the President's message to the American people to promoting the Nation's trade interests abroad.

The President's Cybersecurity Coordinator, working with the Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC), will determine and implement the most efficient and effective method of developing and maintaining interagency situational awareness for policy-related activities. Depending on the effects of the incident, the ICI-IPC, Critical Infrastructure Protection Interagency Policy Committee (CIP-IPC), Domestic Readiness Group (DRG), or other interagency policy groups might be involved in policy coordination activities.

National Security Staff (NSS)

The NSS is the President's principal forum for considering national security and foreign policy matters with his or her senior national security advisors and cabinet officials. Since its inception under President Truman, the NSS's function has been to advise and assist the President on national security and foreign policies. The NSS also serves as the President's principal arm for coordinating these policies among various government agencies.

Office of Management and Budget (OMB)

OMB's predominant mission is to assist the President in overseeing the preparation of the Federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, OMB evaluates the effectiveness of agency programs, policies, and procedures; assesses competing funding demands among agencies; and sets funding priorities. OMB ensures agency reports, rules, testimony, and proposed legislation are consistent with the President's budget and with the administration's policies.

Office of Science and Technology Policy (OSTP)

OSTP provides information, advice, guidance, and assistance, as appropriate, to the President and to Federal departments and agencies with responsibilities for the provision, management, or allocation of communications resources during crises or emergencies in which the exercise of the President's war power functions is not required or permitted by law. The Director, OSTP, also makes recommendations to the President with respect to the test, exercise and evaluation of the capability of existing and planned communications systems, networks or facilities to meet national security or emergency preparedness requirements. The Director of OSTP reports the results of any such tests or evaluations and any recommended remedial actions to the President and National Security Council (NSC). In addition, OSTP advises the President on the effects of science and technology on domestic and international affairs. OSTP serves as a source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal Government. OSTP leads an interagency effort to develop and implement sound science and technology policies and budgets. OSTP works with the private sector to ensure Federal investments in science and technology contribute to economic prosperity, environmental quality, and national security.

Department of Homeland Security (DHS)

DHS is a Cabinet department of the U.S. Federal Government. Its mission is to lead the unified national effort to secure America. DHS aims to prevent and deter terrorist attacks and protect against and respond to threats and hazards to the Nation. DHS seeks to secure national borders while welcoming lawful immigrants, visitors, and trade.

DHS Office of Cybersecurity and Communications (CS&C)

- CS&C, part of the National Protection and Programs Directorate (NPPD), works cooperatively to secure and ensure the availability of cyber and telecommunications infrastructure. Three main organizations under CS&C are the National Cyber Security Division (NCSD), National Communications System (NCS), and Office of Emergency Communications.
- CS&C operates the DHS National Cybersecurity and Communications Integration Center (NCCIC), which co-locates and coordinates the missions of the U.S. Computer Emergency Readiness Team (US-CERT), the National Coordinating Center for Telecommunications (NCC), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the National Cyber Security Center (NCSC), elements of the Office of Intelligence and Analysis (I&A), and other organizations.

DHS National Cybersecurity and Communications Integration Center (NCCIC)

- The NCCIC is a 24x7 integrated cybersecurity and communications operations center. It serves as a centralized location where the operational elements involved in cyber response activities are physically and virtually co-located. The NCCIC is staffed and structured to be an "always ready" multiagency incident response center. During steady-state operations, the NCCIC will utilize its co-located elements and outreach mechanisms to bring all appropriate information together to form a common operational picture and to support a coordinated incident response. Co-located elements include the following:
  - **National Coordinating Center for Telecommunications (NCC):** The NCC is the joint telecommunications industry/Federal operation established by the NCS to assist in the initiation, coordination, restoration, and reconstitution of National Security and Emergency Preparedness (NS/EP) telecommunications services or facilities.
  - **U.S. Computer Emergency Readiness Team (US-CERT):** US-CERT is a partnership between DHS and the public and private sectors. US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration among State, Local, Tribal and Territorial governments, industry, and international partners. US-CERT interacts with Federal agencies, industry, the research community, State, Local, Tribal and Territorial governments, and other entities to disseminate reasoned and actionable cybersecurity information to the public. US-CERT also provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the U.S. Government about cybersecurity.
  - **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT):** ICS-CERT provides focused operational capabilities for defending control system environments against emerging cyber threats. ICS-CERT provides efficient coordination of control systems-related security incidents and information sharing with Federal, State, Local, Tribal and Territorial agencies and organizations; the Intelligence Community (IC); private sector constituents, including vendors, owners, and operators; and international and private sector CERTs. ICS-CERT leads this effort by responding to and

analyzing control systems-related incidents, conducting vulnerability and malware analysis, providing onsite support for forensic investigations, and providing situational awareness in the form of actionable intelligence and reports.

- **National Cyber Security Center (NCSC):** The NCSC is responsible for coordinating and integrating information to provide cross-domain situational awareness; performing reporting and analysis for senior DHS and national policymakers on the strategic state of U.S. cybersecurity; and fostering collaboration and a shared situational awareness among collaborating cybersecurity centers. The NCSC works to provide a cross-organizational information sharing framework to foster situational awareness and allow for a united cyber incident response. The NCSC also provides analytic support and integrated incident response planning and convenes and manages the after-action cyber incident investigative capability emulating collaborative models.

National Communications System (NCS)

The NCS assists the President, NSC, Homeland Security Council, Director of OSTP, and Director of OMB in exercising the communications functions and responsibilities set forth in Section 2 of Executive Order 12472, as amended, and in coordinating the planning for and provision of NS/EP communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. The NCS also serves as a focal point for joint industry-government, national security, and emergency preparedness communications planning. The NCS conducts unified planning and operations to coordinate the development and maintenance of an effective and responsive capability for meeting the domestic and international NS/EP communications needs of the Federal Government. Further, it leads and manages the joint industry-government NCC, which assists in the initiation, coordination, restoration, and reconstitution of NS/EP communications services or facilities under all conditions of crisis or emergency.

National Operations Center (NOC)

The NOC serves as the primary national hub for situational awareness and operations coordination across the Federal Government for incident management. The NOC provides the Secretary of Homeland Security and other principals with information necessary to make critical national-level incident management decisions.

DHS Office of Infrastructure Protection (IP)

DHS IP is responsible for coordinating the national effort to reduce risk to the Nation's critical infrastructure and key resources (CIKR) posed by acts of terrorism and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.

National Infrastructure Coordinating Center (NICC)

As an IP element of the NOC, the NICC monitors the Nation's CIKR on an ongoing basis. During an incident, the NICC provides a coordinating forum to share information across CIKR sectors through appropriate information sharing entities.

National Response Coordination Center (NRCC)

As a component of the NOC, the NRCC serves as the DHS/Federal Emergency Management Agency (FEMA) primary operations center responsible for national incident response and recovery, as well as national resource coordination. As a 24x7 operations center, the NRCC monitors potential or developing incidents and supports the efforts of regional and field components.

Office of Intelligence and Analysis (I&A)

I&A is a member of the IC and ensures that information related to homeland security threats is collected, analyzed, and disseminated to the full spectrum of homeland security customers in DHS; at State, Local, and Tribal levels; in the private sector; and in the IC. I&A works closely with DHS component intelligence organizations and State, Local, Tribal, Territorial, and private sector entities to ensure nontraditional streams of information are fused with traditional IC sources to provide a complete assessment of threats to the Nation.

U.S. Secret Service (USSS)

- The USSS is a Federal law enforcement agency with headquarters in Washington, DC. The USSS was established in 1865 solely to suppress the counterfeiting of U.S. currency. Today, Congress mandates the agency to carry out dual missions: (1) protection of national and visiting foreign leaders and (2) criminal investigations.
- The USSS has established a network of 29 domestic and international Electronic Crimes Task Forces (ECTF) to combine the resources of academia; the private sector; and Federal, State, and Local law enforcement agencies to combat computer-based threats to the U.S. financial payment systems and critical infrastructures. In addition, these combined resources allow ECTF to identify and address potential cyber vulnerabilities before the criminal element exploits them. This proactive approach has successfully prevented cyber attacks that otherwise would have resulted in large-scale financial losses for the American public and U.S.-based companies or disruption of critical infrastructures. More information is available at http://www.secretservice.gov/ectf.shtml.
- **Electronic Crimes Special Agent Program (ECSAP):** A central component of the USSS's cybercrime investigations is the ECSAP. This program comprises 1,148 special agents deployed in more than 98 offices throughout the world. These agents have received extensive training in forensic identification, preservation, and retrieval of electronically stored evidence. The ECSAP program was established to provide special agents basic and advanced computer forensic training. ECSAP agents are trained to conduct computer forensic examinations of electronic evidence obtained from computers, personal data assistants (PDA), electronic organizers, telecommunication devices, and other forms of electronic media.
- **National Computer Forensic Institute (NCFI):** The NCFI is the result of a partnership among the USSS, DHS, and the State of Alabama. The goal of this facility is to provide training for a variety of electronic crimes investigations to the Nation's State and Local law enforcement partners. This program offers State and Local law enforcement officials the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and conduct basic electronic crimes investigations. The USSS provides this training at no cost. Since opening on May 19, 2008, the USSS has provided critical training to 564 State and Local law enforcement officials representing more than 300 agencies from 49 States and two U.S. Territories. For more information, visit www.ncfi.ussss.gov.
- **Cell Phone Forensic Facility:** The ECSAP established a partnership with the University of Tulsa, Digital Forensic Laboratory Center of Information Security, to create a Cell Phone Forensic Facility. The facility expands the ability of law enforcement to pursue a broader range of digital forensics, specifically involving cellular telephones, PDAs, and skimmers. The University supplies a qualified set of interns who specialize in information technology (IT) and digital forensics.

- The USSS maintains a liaison to US-CERT within the NCCIC.

U.S. Immigration and Customs Enforcement (ICE)

- ICE is a Federal law enforcement agency with its headquarters in Washington, DC. ICE is the largest investigative agency in DHS. Formed in 2003 as part of the Federal Government's response to the 9/11 attacks, ICE's mission is to protect the security of the American people and homeland by vigilantly enforcing the Nation's immigration and customs laws. With more than 19,000 employees in more than 400 offices in the United States and around the world, ICE plays a vital role in DHS's layered defense approach to protecting the Nation.
- ICE comprises two operating divisions: Homeland Security Investigations (HSI) and Enforcement and Removal Operations (ERO).
- HSI is responsible for investigating a range of issues that may threaten national security. HSI uses its legal authority to investigate issues such as narcotics, weapons, and other types of smuggling; financial crimes; cybercrime; export enforcement issues; immigration crime; human rights violations; and human smuggling. ICE special agents also conduct investigations aimed at protecting critical infrastructure industries that are vulnerable to sabotage, attack, or exploitation.
- ICE's Office of International Affairs (OIA), part of HSI, is a critical asset in this mission. OIA has more than 60 foreign offices and the broadest international footprint within DHS. ICE OIA offices work with foreign counterparts to identify and combat criminal organizations before they can adversely affect the United States. ICE OIA enhances national security by conducting and coordinating international investigations involving transnational criminal organizations, facilitating domestic ICE investigations overseas, and serving as ICE's liaison to foreign counterparts in Local government and law enforcement.
- The ICE Cyber Crime Center was established in 1997 to combat crimes committed on, or facilitated by, the Internet. It brings together highly technical assets dedicated to conducting trans-border criminal investigations of Internet-related crimes within the ICE portfolio of immigration and customs authorities. It is is responsible for identifying and targeting any cybercrime activity in which ICE has jurisdiction. It's current mission is fourfold: (1) keep pace with emerging computer technology and Internet processes; (2) proactively use these new technologies to combat criminal activity and address vulnerabilities created by the Internet; (3) disseminate to field offices and worldwide law enforcement and intelligence organizations the most current trends, risks, procedures, lessons learned, and investigative leads; and (4) support investigations into online criminal activities and vulnerabilities with state-of-the-art cyber investigative methods and forensic techniques. To accomplish this mission, the Cyber Crime Center's assets are divided into four sections: the Child Exploitation Section, Cyber Crimes Section, Cyber Training Section, and Computer Forensics Section.

Office of Public Affairs

Upon activation of Emergency Support Function -15 (ESF #15) by the DHS Assistant Secretary for Public Affairs, Federal external affairs resources will be utilized to conduct sustained operations in support of the Assistant Secretary for CS&C's efforts during a Significant Cyber Incident requiring a coordinated Federal response. DHS Public Affairs provides accurate, coordinated, and timely information to affected audiences, including governments, media, the private sector, and the local populace.

National Joint Information Center (NJIC)

The DHS NJIC serves as the Federal incident communications coordination center during incidents. The following conference lines are used to coordinate public affairs:

- **National Incident Communications Conference Line (NICCL):** The NICCL is a standing conference line designated, maintained, and supported by DHS Public Affairs as the primary means for interagency incident communications information sharing during an incident requiring Federal coordination. DHS Public Affairs provides guidance to Federal interagency public affairs headquarters staffs and affected authorities through the NICCL.
- **State Incident Communications Conference Line (SICCL):** The SICCL is a dedicated Federal-State incident communications conference line also designated by DHS Public Affairs to facilitate the inclusion, transmission, and exchange of incident management information and messaging to all States and Territories.
- **Private Sector Incident Communications Conference Line (PICCL):** The PICCL is a standing line for use by CIKR incident communications coordinators. Access information will be coordinated and disseminated by DHS Infrastructure Protection and DHS Public Affairs to provide timely public information to the CIKR sectors during an incident requiring Federal coordination and response.

Department of Defense (DOD)

DOD maintains and employs Armed Forces to—

- Support and defend the Constitution of the United States against all enemies, foreign and domestic
- Ensure, by timely and effective military action, the security of the United States, its possessions, and areas vital to its interest
- Uphold and advance the national policies and interests of the United States.

U.S. Strategic Command (USSTRATCOM)

USSTRATCOM directs the operation and defense of the Defense Information Grid to assure timely and secure Net-Centric capabilities across strategic, operational, and tactical boundaries in support of DOD's full spectrum of warfighting, intelligence, and business missions.

U.S. Cyber Command (USCYBERCOM)

USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified DOD information networks and to prepare to (and when directed) conduct full-spectrum military cyberspace operations to enable actions in all domains, ensure freedom of action in cyberspace for the United States and its allies, and deny the same to adversaries. USCYBERCOM is a subordinate command of USSTRATCOM.

Network Warfare/Global Network Operations Joint Operation Center

The Network Warfare/Global Network Operations Joint Operation Center directs the operation and defense of the Global Information Grid to assure timely and secure Net-Centric capabilities across strategic, operational, and tactical boundaries in support of DOD's full spectrum of warfighting, intelligence, and business missions.

Department of Defense Cyber Crime Center (DC3)

DC3 delivers digital forensics and multimedia laboratory services, cyber technical training, and digital forensics research development test and evaluation (RDT&E) to a range of DOD customers, in addition to cyber analysis for investigative, Information Assurance (IA), and information operations requirements. Supported organizations and requirements include DOD

law enforcement and counterintelligence (LE&CI) agencies, counterterrorism (CT) requirements, network defenders and information operations support, document and media exploitation (DOMEX) requirements, inspectors general requests, and safety mishap boards. DC3, designated as a national cyber center under National Security Presidential Directive 54 (NSPD-54), executes these functions through three core directorates and two special organizations. The three core directorates are the Defense Computer Forensics Lab (DCFL), Defense Cyber Investigations Training Academy (DCITA), and Defense Cyber Crime Institute (for RDT&E). The two special organizations are the National Cyber Joint Task Force—Analytical Group, which DC3 staffs and operates as part of an interagency collaboration under the overall cognizance of the Federal Bureau of Investigation (FBI); and the DOD Collaborative Information Sharing Environment (DCISE), which is DOD's operational focal point for developing and disseminating classified and unclassified cyber threat reporting to Defense Industrial Base (DIB) partners and for conducting analysis and diagnostics on DIB partners' reported events.

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

The NSA/CSS is the U.S. Government's lead for cryptologic work in Signals Intelligence (SIGINT)/Computer Network Exploitation (CNE), IA, and Network Threat Operations. The NSA/CSS Threat Operations Center (NTOC) is the primary NSA/CSS partner for DHS response to cyber incidents. The NTOC establishes real-time network awareness and threat characterization capabilities to forecast, alert, and attribute malicious activity and enable the coordination of Computer Network Operations. The primary operational functions of NTOC include creating and maintaining time-sensitive capabilities to determine and disseminate the configuration and activities of networks of interest; characterizing and reporting cyber foreign threats to networks of interest in accordance with NSA's mission to predict, detect, defeat, and attribute exploitations and attacks; conducting 24x7 detection, alert, and incident response services to defend DOD unclassified networks; providing technical assistance, upon request and as appropriate, to Federal entities; and supporting collaborative planning and Computer Network Operations (by NSA/CSS; USSTRATCOM; and the broader community of the United States, its allies, and its mission partners).

Assistant Secretary of Defense for Networks and Information Integration and Department of Defense Chief Information Officer (ASD (NII)/DOD CIO)

The ASD(NII)/DOD CIO oversees the DIB Cybersecurity and IA (CS/IA) activities, including related DOD C3 activities. DOD integrates DIB CS/IA activities into the Defense Critical Infrastructure Program (DCIP) and provides DIB CS/IA subject matter expertise for the DIB sector under the DHS NIPP.

U.S. Northern Command (USNORTHCOM)

USNORTHCOM anticipates and conducts homeland defense and civil support operations within its assigned area of responsibility to defend, protect, and secure the United States and its interests. USNORTHCOM plans, organizes, and executes homeland defense and civil support missions. The command is assigned forces whenever necessary to execute missions, as ordered by the President or Secretary of Defense.

Department of Justice (DOJ)

DOJ's mission is to enforce the law and defend the interests of the United States according to the law; ensure public safety against threats, both foreign and domestic; provide Federal leadership in preventing and controlling crime; seek just punishment for those guilty of unlawful behavior; and ensure fair and impartial administration of justice for all Americans.

Federal Bureau of Investigation (FBI)

The FBI's mission is to protect and defend the United States against terrorist and foreign intelligence threats and to enforce the criminal laws of the United States. The FBI has jurisdiction over violations of more than 200 categories of Federal law.

National Cyber Investigative Joint Task Force (NCIJTF)

The FBI leads the NCIJTF, which is a multiagency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations. The NCIJTF determines the identity, location, intent, motivation, capabilities, alliances, funding, and methodologies of cyber threat groups and individuals necessary to support the U.S. Government's full range of options across all elements of national power.

Criminal Division

The Criminal Division develops, enforces, and supervises the application of all Federal criminal laws.

National Security Division (NSD)

NSD's mission is to combat terrorism and other threats to national security. NSD's organizational structure is designed to ensure greater coordination and unity of purpose between prosecutors and law enforcement agencies, on the one hand, and intelligence attorneys and the Intelligence Community, on the other, thus strengthening the effectiveness of the federal government's national security efforts.

U.S. Attorney's Office

U.S. Attorneys serve as the Nation's principal litigators under the direction of the Attorney General.

Intelligence Community (IC)

Office of the Director of National Intelligence (DNI)

DNI serves as the head of the IC, overseeing and directing the implementation of the National Intelligence Program and acting as the principal advisor to the President, NSC, and Homeland Security Council for intelligence matters related to national security. Working together with the Principal Deputy DNI (PDDNI) and with the assistance of Mission Managers and four Deputy Directors, the Office of the DNI's goal is to effectively integrate foreign, military, and domestic intelligence in defense of the homeland and of United States interests abroad.

Intelligence Community—Incident Response Center (IC-IRC)

The IC-IRC manages and monitors the IC's networks, including conducting network threat analysis and correlation. It provides 24x7 collection and sharing of cyber event information among the IC.

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

The NSA/CSS is the U.S. Government's lead for cryptologic work in SIGINT, CNE, IA, and Network Threat Operations. The NTOC is the primary NSA/CSS partner for DHS response to cyber incidents. The NTOC establishes real-time network awareness and threat characterization capabilities to forecast, alert, and attribute malicious activity and enable coordination of Computer Network Operations. The primary operational functions of NTOC include creating and maintaining time-sensitive capabilities to determine and disseminate the configuration and activities of networks of interest; characterizing and reporting cyber foreign threats to networks of interest in accordance with NSA's mission to predict, detect, defeat, and attribute exploitations and attacks; conducting 24x7 detection, alert, and incident response services to defend DOD

unclassified networks; providing technical assistance, upon request and as appropriate, to Federal entities; and supporting collaborative planning and Computer Network Operations (by NSA/CSS; USSTRATCOM; and the broader community of the United States, its allies, and its mission partners).

Other Key Executive Departments

Department of Commerce

The Department of Commerce's historical mission is "to foster, promote, and develop the foreign and domestic commerce" of the United States. This mission has evolved, as a result of legislative and administrative additions, to encompass broadly the responsibility to foster, serve, and promote the Nation's economic development and technological advancement.

Department of Energy (DOE)

DOE's overarching mission is to advance the national, economic, and energy security of the United States; promote scientific and technological innovation in support of that mission; and ensure the environmental cleanup of the national nuclear weapons complex.

Department of State

The Department of State is the U.S. Federal executive department responsible for international relations. Among its stated missions is to advance freedom for the benefit of the American people and the international community by helping to build and sustain a more democratic, secure, and prosperous world composed of well-governed States that respond to the needs of their people, reduce widespread poverty, and act responsibly within the international system. The Department of State formulates, coordinates, and provides oversight of foreign policy.

Department of the Treasury (Treasury)

Treasury is the executive agency responsible for promoting economic prosperity and ensuring the financial security of the United States. Treasury is responsible for a wide range of activities, such as advising the President on economic and financial issues, encouraging sustainable economic growth, and fostering improved governance in financial institutions. Treasury operates and maintains systems that are critical to the Nation's financial infrastructure, such as producing coin and currency, disbursing payments to the American public, collecting revenue, and borrowing funds necessary to run the Federal Government.

Public-Private Partnerships

Communications Infrastructure Information Sharing and Analysis Center (COMMs ISAC)

One function of the NCC is the COMMs ISAC. The COMMs ISAC's mission is to facilitate voluntary collaboration and information sharing among Government and industry in support of Executive Order 12472 and the national critical infrastructure protection goals of Presidential Decision Directive 63 (PDD-63); to gather information on vulnerabilities, threats, intrusions, and anomalies from multiple sources; and to perform analysis with the goal of averting or mitigating impact on the telecommunications infrastructure.

Electricity Sector Information Sharing and Analysis Center (ES-ISAC)

The ES-ISAC serves the electricity sector by facilitating communications between electricity sector participants, the Federal Government, and other critical infrastructures. It is the job of the ES-ISAC to promptly disseminate threat indications, analyses, and warnings, together with interpretations, to help electricity sector participants take protective actions.

Financial Services Information Sharing and Analysis Center (FS-ISAC)

The FS-ISAC's mission, in collaboration with Treasury and the Financial Services Sector Coordinating Council (FSSCC), is to enhance the financial services sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents, and to serve as the primary communications channel for the sector. The FS-ISAC is the designated operational arm of the FSSCC. The FS-ISAC supports the protection of the U.S. financial services sector by assisting both FSSCC and Treasury in identifying, prioritizing, and coordinating the protection of critical financial services, infrastructure services, and key resources. It also facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and practices.

Council of Information Sharing and Analysis Centers (ISAC)

The mission of the Council of ISACs is to advance the physical security and cybersecurity of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and government. ISACs work together to better understand cross-industry dependencies and account for them in emergency response planning.

Information Technology Information Sharing and Analysis Center (IT-ISAC)

The IT-ISAC is a trusted community of security specialists from companies across the IT industry. These specialists are dedicated to protecting the IT infrastructure that propels today's global economy by identifying threats and vulnerabilities to the infrastructure and sharing best practices on how to quickly and properly address them.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

The MS-ISAC's mission is to provide a common mechanism for raising the level of cybersecurity readiness and response in each State and among Local, Tribal, and Territorial governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between and among the States and Local, Tribal, and Territorial governments.

Water Information Sharing and Analysis Center (WaterISAC)

The WaterISAC collects and reviews infrastructure protection information from government and private sources to share with its subscribers. Analysts tap into classified intelligence and open-source information 24 hours a day to track security incidents across the world. WaterISAC is the official communications arm of the Water Sector Coordinating Council and is at the forefront of disseminating cybersecurity-centric threat information to the water sector.

Sector Coordinating Councils (SCC)/Government Coordinating Councils (GCC)

SCCs and GCCs operate under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework, which facilitates effective coordination between Federal infrastructure protection programs and infrastructure protection activities of State, Local, Tribal, and Territorial governments and the private sector. The CIPAC provides a forum in which government and private sector partners can engage in a broad spectrum of activities to support and coordinate CIKR protection.

InfraGard

InfraGard is a partnership among the FBI, other governmental entities, and the private sector. The InfraGard National Membership Alliance is an association of businesses, academic institutions, State and Local law enforcement agencies, and other participants that enables the

sharing of knowledge, expertise, information, and intelligence related to the protection of U.S. CIKR against physical and cyber threats.

Electronic Crimes Task Forces (ECTF)

The USSS coordinates with 29 ECTF to combine the resources of academia; the private sector; and Local, State, and Federal law enforcement agencies to combat computer-based threats to the Nation's financial payment systems and critical infrastructures.

Department of Defense's Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) Program

The Deputy Secretary of Defense directed the establishment of the DOD DIB CS/IA pilot program in 2007 to address cybersecurity risks to the unclassified networks of cleared defense companies that process or maintain DOD program information. DOD DIB CS/IA provides a mechanism, including a secure network, for cyber threat information sharing, cyber incident reporting, and cyber intrusion damage assessment under a voluntary framework agreement between DOD and companies at the corporate level.

[This page intentionally left blank.]

Appendix O: Acronym List

Acronym	Meaning
ASD (NII)/DOD CIO	Assistant Secretary of Defense for Networks and Information Integration and Department of Defense Chief Information Officer
CAT	Crisis Action Team
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulations
CII	Critical Infrastructure Information
CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Officers
CIPAC	Critical Infrastructure Partnership Advisory Council
CIP-IPC	Critical Infrastructure Protection Interagency Policy Committee
CISO	Chief Information Security Officers
CNCI	Comprehensive National Cybersecurity Initiative
CNE	Computer Network Exploitation
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COMMs ISAC	Communications Infrastructure Information Sharing and Analysis Center
CONOPS	Concept of Operations
CS&C	Office of Cybersecurity and Communications
CS/IA	Cybersecurity and Information Assurance
CSIRT	Computer Security Incident Response Team
CSS	Central Security Service
CT	Counterterrorism
DC3	Department of Defense Cyber Crime Center
DCFL	Defense Computer Forensics Lab
DCIP	Defense Critical Infrastructure Program
DCISE	DOD Collaborative Information Sharing Environment
DCITA	Defense Cyber Investigations Training Academy
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DIB CS/IA	Defense Industrial Base Cybersecurity and Information Assurance

DNI	Office of the Director of National Intelligence
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOMEX	Document and Media Exploitation
DOS	Department of State
DRG	Domestic Readiness Group
DRO	Office of Detention and Removal Operations
DSCA	Defense Support of Civil Authorities
ECSAP	Electronic Crimes Special Agent Program
ECTF	Electronic Crimes Task Forces
EOP	Executive Office of the President
ERO	Enforcement and Removal Operations
ESF	Emergency Support Function
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council
GCC	Government Coordinating Council
HSA	Homeland Security Advisor
HSI	Homeland Security Investigation
HSPD	Homeland Security Presidential Directive
I&A	Office of Intelligence and Analysis
IA	Information Assurance
IC	Intelligence Community
ICE	Immigration and Customs Enforcement
ICI-IPC	Information and Communications Infrastructure Interagency Policy Committee

IC-IRC	Intelligence Community—– – Incident Response Center
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IGA	Office of Intergovernmental Affairs
IMT	Incident Management Team
IP	Office of Infrastructure Protection
IR	Interagency Report
ISAC	Information Sharing and Analysis Centers
IT	Information Technology
IT-ISAC	Information Technology Information Sharing and Analysis Center
JP	Joint Publication
JTF-GNO	Joint Task Force—-Global Network Operations
JTRB	Joint Telecommunications Resource Board
LE&CI	Law Enforcement and Counterintelligence
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCC	National Coordinating Center for Telecommunications
NCCIC	National Cybersecurity and Communications Integration Center
NCFI	National Computer Forensic Institute
NCIJTF	National Cyber Investigative Joint Task Force
NCIRP	National Cyber Incident Response Plan
NCRAL	National Cyber Risk Alert Level
NCS	National Communications System
NCSC	National Cyber Security Center
NCSD	National Cyber Security Division
NGO	Nongovernmental Organization
NICC	National Infrastructure Coordinating Center
NICCL	National Incident Communications Conference Line
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute for Standards and Technology
NJIC	National Joint Information Center
NOC	National Operations Center

NPPD	National Protection and Programs Directorate
NRCC	National Response Coordination Center
NRF	National Response Framework
NS/EP	National Security and Emergency Preparedness
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSC	National Security Council
NSD	National Security Division
NSOC	National Security Operations Center
NSPD	National Security Presidential Directive
NSS	National Security Staff
NTIA	National Telecommunications and Information Administration
NTOC	NSA/CSS Threat Operations Center
OASD	Office of the Assistant Secretary of Defense
OI	Office of Investigations
OIA	Office of International Affairs
OMB	Office of Management and Budget
OPS	Office of Operations and Coordination
OSTP	Office of Science and Technology Policy
PCII	Protected Critical Infrastructure Information
PDA	Personal Data Assistant
PDD	Presidential Decision Directive
PDDNI	Principal Deputy Director of National Intelligence
PICCL	Private Sector Incident Communications Conference Line
POTUS	President of the United States
RDT&E	Research Development Test and Evaluation
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SFLEO	Senior Federal Law Enforcement Official
SICCL	State Incident Communications Conference Line
SIGINT	Signals Intelligence

SOP	Standard Operating Procedure
SP	Special Publication
SSA	Sector Specific Agency
SWO	Senior Watch Officer
U.S.C.	United States Code
UCG	Unified Coordination Group
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USCYBERCOM	United States Cyber Command
USNORTHCOM	United States Northern Command
USSS	United States Secret Service
USSTRATCOM	United States Strategic Command
WaterISAC	Water Information Sharing and Analysis Center

245 Murray Lane SW Bldg 410
Mailstop 0640
Washington DC 20528

NCCIC@dhs.gov