Cyber Incident Annex

Coordinating Agencies:

Department of Defense
Department of Homeland Security/Information Analysis and Infrastructure Protection/National Cyber Security Division
Department of Justice

Cooperating Agencies:

Department of Commerce
Department of Energy
Department of Homeland Security
Department of State
Department of Transportation
Department of the Treasury
Intelligence Community
National Institute of Standards and Technology
Office of Management and Budget

Introduction

Purpose

This annex discusses policies, organization, actions, and responsibilities for a coordinated, multidisciplinary, broad-based approach to prepare for, respond to, and recover from cyber-related Incidents of National Significance impacting critical national processes and the national economy.

Scope

This annex describes the framework for Federal cyber incident response coordination among Federal departments and agencies and, upon request, State, local, tribal, and private-sector entities. The Cyber Incident Annex is built primarily upon the National Cyberspace Security Response System (NCSRS), described in the National Strategy to Secure Cyberspace. The NCSRS is a public-private architecture that provides mechanisms for rapid identification, information exchange, response, and remediation to mitigate the damage caused by malicious cyberspace activity.

This framework may be utilized in any Incident of National Significance with cyber-related issues, including significant cyber threats and disruptions; crippling cyber attacks against the Internet or critical infrastructure information systems; technological emergencies; or Presidentially declared disasters.

This annex describes the specialized application of the National Response Plan (NRP) to cyber-related Incidents of National Significance. Cyber-related Incidents of National Significance may result in activation of both ESF #2 – Communications and the Cyber Incident Annex.

When processes in both annexes are activated, the Department of Homeland Security/Information Analysis and Infrastructure Protection/National Cyber Security Division (DHS/IAIP/NCSD) continues its responsibilities under this annex and also fulfills its responsibilities as described in ESF #2.

Policies

- The procedures discussed in this annex are governed by Federal Government cyber security principles.
- This annex complements the National Plan for Telecommunications Support in Non-Wartime Emergencies, hereafter referred to as the National Telecommunications Support Plan (NTSP).
- This annex is implemented within the framework and operating principles of the NRP and pursuant to the following authorities:
  - The Enhancement of Non-Federal Cyber Security, The Homeland Security Act (Section 223 of P.L. 107-276)

- Homeland Security Presidential Directive-5 (HSPD-5)
- Homeland Security Presidential Directive-7 (HSPD-7)
- Federal Information Security Management Act (FISMA)
- Executive Order 12472: The Assignment of National Security Emergency Preparedness Responsibilities for Telecommunications
- Section 706, Communications Act of 1934, as amended (47 U.S.C. 606)
- The 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
- Executive Order 12333: United States Intelligence Activities, as amended
- National Strategy to Secure Cyberspace

Concept of Operations

General

A cyber-related Incident of National Significance may take many forms: an organized cyber attack, an uncontrolled exploit such as a virus or worm, a natural disaster with significant cyber consequences, or other incidents capable of causing extensive damage to critical infrastructure or key assets.

Large-scale cyber incidents may overwhelm government and private-sector resources by disrupting the Internet and/or taxing critical infrastructure information systems. Complications from disruptions of this magnitude may threaten lives, property, the economy, and national security. Rapid identification, information exchange, investigation, and coordinated response and remediation often can mitigate the damage caused by this type of malicious cyberspace activity.

The Federal Government plays a significant role in managing intergovernmental (Federal, State, local, and tribal) and, where appropriate, public-private coordination in response to cyber Incidents of National Significance. Federal Government responsibilities include:

- Providing indications and warning of potential threats, incidents, and attacks;
- Information-sharing both inside and outside the government, including best practices, investigative information, coordination of incident response, and incident mitigation;
- Analyzing cyber vulnerabilities, exploits, and attack methodologies;
- Providing technical assistance;
- Conducting investigations, forensics analysis, and prosecution;
- Attributing the source of cyber attacks;
- Defending against the attack; and
- Leading national-level recovery efforts.

These activities are the product of, and require, a concerted effort by Federal, State, local, and tribal governments, and nongovernmental entities such as private industry and academia.

Organization

Interagency Incident Management Group (IIMG): Upon notification of a potential or actual incident, the Secretary of Homeland Security may activate the IIMG. The IIMG is tailored with required DHS components and Federal departments for a cyber incident. The National Cyber Response Coordination Group (NCRCG) provides subject-matter expertise related to the cyber threat, analysis, and recommendations to the IIMG.

National Cyber Response Coordination Group: The NCRCG is comprised of senior representatives from Federal agencies that have roles and responsibilities related to preventing, investigating, defending against, responding to, mitigating, and assisting in the recovery from cyber incidents and attacks. In the event of a cyber-related Incident of National Significance requiring Federal response and interagency coordination, the NCRCG is convened to harmonize operational efforts and facilitate information-sharing.

The NCRCG is an interagency forum where organizations responsible for a range of activities (technical response and recovery, law enforcement, intelligence, and defensive measures) coordinate for the purposes of preparing for and executing an efficient and effective response to an incident.

The NCRCG performs the following functions:

- Provides input to member agency and department heads and the IIMG on cyber security issues, incidents, and threats;
- Assists in reviewing threat assessments and providing strategic situational awareness and decision support across the national cyber incident management spectrum, including prevention, preparedness, response, and recovery;
- Synthesizes information, frames policy issues, and recommends actions—including use or allocation of Federal resources—for agency and department heads, the IIMG, and other appropriate officials; and
- As appropriate, supports the Executive Office of the President.

During actual or potential Incidents of National Significance, the NCRCG coordinates with the Homeland Security Operations Center (HSOC) in disseminating critical information to and from government and nongovernment sources such as information-sharing mechanisms, academia, industry, and the public. The NCRCG leverages existing resources of DHS/IAIP/NCSD/U.S. Computer Emergency Readiness Team (US-CERT) in this coordination and outreach activity.

- **U.S. Computer Emergency Readiness Team:** The US-CERT, in coordination with the Office of Management and Budget (OMB), coordinates warnings among Federal departments and agencies. The US-CERT maintains a 24/7 operations center with connectivity to all major Federal cyber operations centers and private-sector Internet service providers, information-sharing mechanisms, and vendors. The US-CERT, in concert with the HSOC, acts as a focal point to collect and disseminate, to the appropriate audiences, information received from public and private sector sources. Also, DHS/IAIP/NCSD/US-CERT provides technical and operational support to the IIMG, and interacts with private and public sectors on a continuous basis throughout the extent of the incident.
- **Intelligence Community – Incident Response Center (IC-IRC):** The Intelligence Community operates the IC-IRC, a 24/7 operation that facilitates the sharing of cyber event information among members of the Intelligence Community in order to protect the Intelligence Community's ability to collect, analyze, and disseminate intelligence via its networks. The IC-IRC is responsible for coordinating with other incident response organizations including US-CERT and the HSOC, enabling such organizations to leverage the Intelligence Community's analytic capabilities for providing advanced indications of potential threats.
- **Department of Defense (DOD):** DOD operates a network of Computer Emergency Response Teams which are staffed 24/7. These teams are coordinated by the Joint Task Force–Global Network Operations (JTF-GNO) to identify, mitigate, and, if necessary, respond to cyber attacks. U.S. Strategic Command (USSTRATCOM) and JTF-GNO also provide continuous intelligence analysis of cyber threats. Finally, the Law Enforcement/Counter Intelligence Center, located at the JTF-GNO, brings together DOD's law enforcement and counterintelligence organizations in response to cyber incidents.

Actions

Pre-Incident

Federal departments and agencies maintain computer incident response capabilities that can rapidly respond to cyber incidents on their networks, including events of prolonged duration. Law enforcement, the Intelligence Community, and DOD also maintain mechanisms that improve the Nation's readiness to address cyber incidents. The Department of Justice (DOJ) has a network of prosecutors trained in handling cybercrime. The Federal Bureau of Investigation (FBI) and the U.S. Secret Service (DHS/USSS) have agents that specialize in high-tech investigations. Law enforcement's international cybercrime network enables investigators rapidly to obtain electronic data and evidence from foreign countries.

Notification and Activation Procedures

Procedures in this annex are implemented when it is determined that a cyber-related Incident of National Significance is imminent or underway. The NCRCG is convened and immediately notifies the DHS/IAIP/NCS. Notification is made through established communications channels that exist between the Federal Government, nongovernmental entities, and the public. Such channels of communication include:

- **National Cyber Alert System:** This system provides an infrastructure, managed by US-CERT, for relaying timely and actionable computer security update and warning information to all users.

- **Homeland Security Information Network (HSIN) Joint Regional Information Exchange System:** This communications network provides States and major urban areas real-time interactive connectivity with the HSOC through a secure system carrying information on a Sensitive-but-Unclassified (SBU) level to all users.

- **Homeland Security Operations Center:** This is the primary national-level hub for domestic incident management communications and operations.

- **Cyber Warning Information Network:** This network provides out-of-band (i.e., not dependent on Internet or PSTN) connectivity to government and industry participants. The network is engineered to provide a reliable and survivable network capability.

- **HSIN/US-CERT Portal:** This is a secure collaboration tool for private and public sectors to actively converse about cyber security vulnerabilities, exploits, and incidents in a trusted environment among and between members.

- **US-CERT Public Web Site:** This Web site provides the primary means for US-CERT to convey information to the public at large. The site includes relevant and current information on cyber security issues, current cyber activity, and vulnerability resources.

Initial Actions

DHS/IAIP/NCSD, other elements of DHS, the Intelligence Community, FBI, DOD, and other Government agencies work closely together in the NCRCG and individually to coordinate response during a cyber incident or attack, identify those responsible, and otherwise respond appropriately.

When a cyber Incident of National Significance occurs, DHS/IAIP/NCSD, through the NCRCG, coordinates with the National Communications System (NCS) and supports the Joint Telecommunications Resources Board (JTRB).

The US-CERT Operations Center tracks potential cyber incidents and, when warranted, reports them to the NCRCG. The NCRCG notifies the HSOC of cyber-related incidents. The NCRCG, in coordination with the IIMG, makes recommendations to the Secretary of Homeland Security, who is responsible for designating Incidents of National Significance. The activities described in this annex are implemented when a cyber-related Incident of National Significance is imminent or underway.

Ongoing Actions

DHS coordinates technical and other assistance with and/or to other Federal agencies and, upon request, to the State, local, and tribal governments and the private sector for response to major failures of critical information systems. Requests for Federal assistance are handled as described in section V of the NRP.

Challenges and Considerations

The response to and recovery from a cyber Incident of National Significance must take into account existing challenges to the effective management of significant cyber incidents and the resulting physical effects of such cyber incidents and of cyber consequences of physical incidents. Such consideration allows resources to be appropriately channeled into resolving identified challenges. Identifiable challenges include:

- **Management of Multiple Cyber Events:** The occurrence or threat of multiple cyber incidents may significantly hamper the ability of responders to adequately manage the cyber incident. Strategic planning and exercises should be conducted to assist in addressing this problem.
- **Availability and Security of Communications:** A debilitating infrastructure attack could impede communications needed for coordinating response and recovery efforts. A secure, reliable communications system is needed to enable public and private-sector entities to coordinate efforts in the event that routine communications channels are inoperable.
- **Availability of Expertise and Surge Capacity:** Federal agencies must ensure that sufficient technical expertise is developed and maintained within the Government to address the wide range of ongoing cyber attacks and investigations. In addition, the ability to surge technical and analytical capabilities in response to cyber incidents that may occur over a prolonged period must be planned for, exercised, and maintained.
- **Coordination With the Private Sector:** Cyberspace is largely owned and operated by the private sector; therefore, the authority of the Federal Government to exert control over activities in cyberspace is limited.

Responsibilities

Coordinating Agencies

Apart from the NCRCG, certain Federal departments and agencies have core roles and responsibilities related to securing cyberspace and coordinating incident response.

Department of Defense	DOD entities responsible for computer security and computer network defense 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. DOD capabilities include Intelligence components (the National Security Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Organization, and military intelligence components), Defense criminal investigative organizations (law enforcement and counterintelligence), Network Operation Security Centers, and Computer Emergency Response Teams. These entities, in cooperation with other Federal entities, as appropriate, provide attack sensing and warning capabilities, gather and analyze information to characterize the attack and to gain attribution of the cyber threat, participate in information-sharing, offer mitigation techniques, perform network intrusion diagnosis and provide technical expertise. DOD capabilities also include military operational units, which defend the DOD global information grid. DOD can take action to deter or defend against cyber attacks which pose an imminent threat to national security, as authorized by applicable law and policy.
Department of Homeland Security/Infrastructure Analysis and Infrastructure Protection/National Cyber Security Division	DHS/IAIP/NCSD is a focal point for the security of cyberspace for purposes of analysis, warning, information-sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. It facilitates interactions and collaborations (with the exception of investigation and prosecution of cybercrime, military operations to defend the homeland, or other activities identified below) between and among the Federal departments and agencies; State, local, and tribal governments; the private sector; and international organizations. Other Federal departments and agencies with cyber expertise collaborate with and support DHS in accomplishing its mission. DHS/IAIP/NCSD is responsible for preparation for and response to cyber threats, vulnerabilities, and incidents and works closely with the DHS/IAIP/NCS and DHS/USSS in its prevention and protection role. DHS/IAIP/NCSD supports DOJ and other Federal law enforcement agencies in their mission to investigate and prosecute threats to and attacks against cyberspace. DHS/IAIP/NCSD also reports to the Secretary of Homeland Security and the Executive Office of the President, as appropriate, regarding coordination and response related to cyber incidents. DHS/IAIP/NCSD coordinates with the Department of State (DOS) on the notification and resolution of incidents with foreign governments. DHS and DOS coordinate with the interagency community to work with foreign countries and international organizations to strengthen the protection of U.S. critical information infrastructures and those foreign critical information infrastructures on which the United States relies.

Department of Justice/Federal Bureau of Investigation	DOJ and the FBI, working with other law enforcement agencies, lead the national effort to investigate and prosecute cybercrime. 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 U.S. citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States. DOJ, in cooperation with other Federal departments and agencies engaged in activities to protect national security, also coordinates the activities of the other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States. DOJ, working with other law enforcement agencies and the intelligence community, uses its authorities to attribute the source of a cyber attack. Among other things, DOJ works with the private sector in regard to the prevention, investigation, and prosecution of cybercrime. DOJ coordinates with DHS to provide domestic investigative information relevant to DHS analysis of the vulnerability of the cyber infrastructure to terrorist attack or to DHS analysis of terrorist threats against the cyber infrastructure.

Cooperating Agencies

Department of Homeland Security/U.S. Secret Service	DHS/USSS works with the FBI and other law enforcement agencies in helping to lead the national effort to investigate and prosecute cybercrime. DHS/USSS coordinates with DOJ to assist in providing domestic investigative information used in DHS analysis of the vulnerability of the cyber infrastructure to terrorist attacks.
Department of State	DOS coordinates, in conjunction with DHS/IAIP/NCSD, Federal Government efforts in the development and implementation of foreign policies related to cyberspace security. DOS engages in the following activities to support U.S. national cyber security goals and objectives: ▪ Chairs the interagency International Critical Infrastructure Protection Working Group. This group serves as an interagency coordination mechanism on international cyber security matters of a bilateral, multilateral, or international nature. ▪ Participates as a member of the NCRCG to provide advice and assistance on the foreign policy issues related to a cyber incident of national significance. ▪ Manages a cable/message address collective available for use to notify senior foreign leaders of 30 allied and like-minded nations of cyber incidents of international significance. This collective is a vehicle by which the United States can notify senior national-level personnel in select foreign governments of impending cyber incidents; it complements the technical watch and warning notifications distributed by US-CERT.

The Intelligence Community	The Intelligence Community, through the IC-IRC, coordinates and shares information with DOD, US-CERT, and other incident response organizations in order to safeguard the integrity of Intelligence Community networks. The IC-IRC uses procedures to ensure that the Director of Central Intelligence and the President are kept informed of any activity that could jeopardize the ability of the Intelligence Community to accomplish its mission. In the event of a cyber emergency, the Intelligence Community exercises its authorities and uses its resources and expertise to provide foreign threat-based analysis and to assist in efforts to gain attribution regarding a cyber attack.
Other Cooperating Agencies	Other Federal departments and agencies, listed as cooperating agencies, provide cyber-related expertise in support of this annex as requested.

Other Federal Entities

Office of Science and Technology Policy	The Director, Office of Science and Technology Policy (OSTP), is responsible for the coordination of planning for and provision of national security and emergency preparedness communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. The Director, OSTP, chairs the JTRB, which brings together Federal communications policymakers with key authorities during an Incident of National Significance involving communications. The communications-related responsibilities and authorities for OSTP are found in the Communications Act of 1934, Executive Order 12472, ESF #2, and the NTSP.
Homeland Security Council/National Security Council	The Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs provide interagency policy coordination for domestic and international incident management, respectively, as directed by the President.
Office of Management and Budget	OMB, through the Federal Information Security Management Act (FISMA) requirements and with the assistance of US-CERT, chief information officers, and the departments' and agencies' Inspectors General, ensures that the departments and agencies properly employ continuity and recovery plans in response to a cyber incident.
Sector-Specific Agencies	The heads of all Federal departments and agencies, as directed by HSPD-5 and HSPD-7, provide their full and prompt cooperation, resources, and support, as consistent with law, policy, and their own responsibilities for protecting national security.

Other Entities

State, Local, and Tribal Governments	The Federal Government uses available homeland security, emergency management, and other information-sharing mechanisms to provide centrally coordinated sharing of security intelligence and information to the States. In addition, in the event of a cyber Incident of National Significance, State, local, and tribal government entities are encouraged to activate their incident management/response support architecture and coordinate through the national incident management structure, to include requests for the provision of additional resources to address the incident. The ability of States to quickly and effectively augment local response operations may be enhanced through participation in the development of venue-specific cyber incident response plans that include a coordinated advance strategy for receiving, deploying, and/or utilizing preidentified State resources. DHS can assist in the creation of such plans.
Nongovernmental Entities	The Federal Government recognizes that the private and nongovernmental sectors play a central role in preventing, preparing for, responding to, and recovering from cyber incidents. Consequently, the Federal Government, primarily through DHS, maintains multiple lines of communication with the private and nongovernmental sectors to permit the ongoing exchange of vital security information. Information-sharing mechanisms allow critical sectors to share information and to work together to better protect infrastructures across all sectors of society. Through information-sharing mechanisms and associations, information about network vulnerabilities and effective solutions, as well as information related to threats and ways to protect against those threats, is provided to the private and nongovernmental sectors to assist them in achieving a higher level of critical infrastructure protection. In the event of a cyber incident, the Federal Government continues to work with the private sector in a coordinated response. DHS/IAIP/NCSD serves as a focal point for cyberspace security and facilitates interactions and collaborations with nongovernmental and private-sector entities for purposes of analysis, warning, information-sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. The private sector and academia use many security mechanisms and have their own internal cyber security management systems. However, widespread cyber disruption requires high levels of cooperation and sector-specific and cross-sector collaboration. Therefore, the private sector and academia are encouraged to work with sector-specific agencies, information-sharing mechanisms, associations, DHS, and law enforcement through existing mechanisms to ensure that adequate collaboration is conducted. In addition, DOJ and law enforcement authorities continue to work with the private sector with respect to prevention, investigation, and prosecution of cybercrime. For example, entities such as InfraGard and the Electronic Crime Task Forces (ECTFs) work to improve and extend information-sharing between private industry and government (particularly FBI and DHS/USSS, respectively) regarding critical infrastructures. InfraGard and the ECTFs promote ongoing dialogue and timely communication between private industry and Federal law enforcement and enable industry to protect assets and provide information to the Government that can help prevent terrorism and other crimes.