Directive on United States Cyber Incident Coordination

July 26, 2016

Presidential Policy Directive/PPD–41

Subject: United States Cyber Incident Coordination

The advent of networked technology has spurred innovation, cultivated knowledge, encouraged free expression, and increased the Nation's economic prosperity. However, the same infrastructure that enables these benefits is vulnerable to malicious activity, malfunction, human error, and acts of nature, placing the Nation and its people at risk. Cyber incidents are a fact of contemporary life, and significant cyber incidents are occurring with increasing frequency, impacting public and private infrastructure located in the United States and abroad.

United States preparedness efforts have positioned the Nation to manage a broad range of threats and hazards effectively. Every day, Federal law enforcement and those agencies responsible for network defense in the United States manage, respond to, and investigate cyber incidents in order to ensure the security of our information and communications infrastructure. The private sector and government agencies have a shared vital interest in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences. The nature of cyberspace requires individuals, organizations, and the government to all play roles in incident response. Furthermore, effective incident response efforts will help support an open, interoperable, secure, and reliable information and communications infrastructure that promotes trade and commerce, strengthens international security, fosters free expression, and reinforces the privacy and security of our citizens.

While the vast majority of cyber incidents can be handled through existing policies, certain cyber incidents that have significant impacts on an entity, our national security, or the broader economy require a unique approach to response efforts. These significant cyber incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors.

I. Scope

This Presidential Policy Directive (PPD) sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. For significant cyber incidents, this PPD also establishes lead Federal agencies and an architecture for coordinating the broader Federal Government response. This PPD also requires the Departments of Justice and Homeland Security to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities.

II. Definitions

A. *Cyber incident.* An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an

information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

B. *Significant cyber incident.* A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

III. Principles Guiding Incident Response

In carrying out incident response activities for any cyber incident, the Federal Government will be guided by the following principles:

A. *Shared Responsibility.* Individuals, the private sector, and government agencies have a shared vital interest and complementary roles and responsibilities in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.

B. *Risk-Based Response.* The Federal Government will determine its response actions and the resources it brings to bear based on an assessment of the risks posed to an entity, our national security, foreign relations, the broader economy, public confidence, civil liberties, or the public health and safety of the American people.

C. *Respecting affected entities.* To the extent permitted under law, Federal Government responders will safeguard details of the incident, as well as privacy and civil liberties, and sensitive private sector information, and generally will defer to affected entities in notifying other affected private sector entities and the public. In the event a significant Federal Government interest is served by issuing a public statement concerning an incident, Federal responders will coordinate their approach with the affected entities to the extent possible.

D. *Unity of Governmental Effort.* Various government entities possess different roles, responsibilities, authorities, and capabilities that can all be brought to bear on cyber incidents. These efforts must be coordinated to achieve optimal results. Whichever Federal agency first becomes aware of a cyber incident will rapidly notify other relevant Federal agencies in order to facilitate a unified Federal response and ensure that the right combination of agencies responds to a particular incident. State, local, tribal, and territorial (SLTT) governments also have responsibilities, authorities, capabilities, and resources that can be used to respond to a cyber incident; therefore, the Federal Government must be prepared to partner with SLTT governments in its cyber incident response efforts. The transnational nature of the Internet and communications infrastructure requires the United States to coordinate with international partners, as appropriate, in managing cyber incidents.

E. *Enabling Restoration and Recovery.* Federal response activities will be conducted in a manner to facilitate restoration and recovery of an entity that has experienced a cyber incident, balancing investigative and national security requirements, public health and safety, and the need to return to normal operations as quickly as possible.

IV. Concurrent Lines of Effort

In responding to any cyber incident, Federal agencies shall undertake three concurrent lines of effort: threat response; asset response; and intelligence support and related activities. In addition, when a Federal agency is an affected entity, it shall undertake a fourth concurrent

line of effort to manage the effects of the cyber incident on its operations, customers, and workforce.

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

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

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

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

D. An affected Federal agency shall engage in a variety of efforts to manage the impact of a cyber incident, which may include maintaining business or operational continuity; addressing adverse financial impacts; protection of privacy; managing liability risks; complying with legal and regulatory requirements (including disclosure and notification); engaging in communications with employees or other affected individuals; and dealing with external affairs (e.g., media and congressional inquiries). The affected Federal agency will have primary responsibility for this line of effort.

   When a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity. The relevant sector-specific agency (SSA) will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

V. Architecture of Federal Government Response Coordination for Significant Cyber Incidents[1]

[1] Additional details regarding the Federal Government's coordination architecture for significant cyber incidents are contained in an annex to this PPD.

In order to respond effectively to significant cyber incidents, the Federal Government will coordinate its activities in three ways:

A. National Policy Coordination[2]

The Cyber Response Group (CRG), in support of the National Security Council (NSC) Deputies and Principals Committees, and accountable through the Assistant to the President for Homeland Security and Counterterrorism (APHSCT) to the NSC chaired by the President, shall coordinate the development and implementation of United States Government policy and strategy with respect to significant cyber incidents affecting the United States or its interests abroad.

B. National Operational Coordination

1. Agency Enhanced Coordination Procedures. Each Federal agency that regularly participates in the CRG, including SSAs, shall establish and follow enhanced coordination procedures as defined in the annex to this PPD in situations in which the demands of responding to a significant cyber incident exceed its standing capacity.

2. Cyber Unified Coordination Group. A Cyber Unified Coordination Group (UCG) shall serve as the primary method for coordinating between and among Federal agencies in response to a significant cyber incident as well as for integrating private sector partners into incident response efforts, as appropriate. A Cyber UCG shall be formed at the direction of the NSC Principals Committee, Deputies Committee, or the CRG, or when two or more Federal agencies that generally participate in the CRG, including relevant SSAs, request its formation. A Cyber UCG shall also be formed when a significant cyber incident affects critical infrastructure owners and operators identified by the Secretary of Homeland Security as owning or operating critical infrastructure for which a cyber incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

   A Cyber UCG will normally consist of Federal lead agencies for threat response, asset response, and intelligence support, but will also include SSAs, if a cyber incident affects or is likely to affect sectors they represent. In addition, as required by the scope, nature, and facts of a particular significant cyber incident, a Cyber UCG may include participation from other Federal agencies, SLTT governments, nongovernmental organizations, international counterparts, or the private sector.

   Following the formation of a Cyber UCG, Federal agencies responding to the incident shall assign appropriate senior executives, staff, and resources to execute the agency's responsibilities as part of a Cyber UCG. The Cyber UCG is intended to result in unity of effort and not to alter agency authorities or leadership, oversight, or command responsibilities. Unless mutually agreed upon between agency heads or their designees, and consistent with applicable legal authorities such as the Economy Act of 1932 (31 U.S.C. 1535), Federal departments and agencies will maintain operational control over their respective agency assets.

3. Federal lead agencies. In order to ensure that the Cyber UCG achieves maximum effectiveness in coordinating responses to significant cyber incidents, the following agencies shall serve as Federal lead agencies for the specified line of effort:

[2] This sub-section supersedes NSPD–54/HSPD–23, paragraph 13, concerning the National Cyber Response Coordination Group.

a. In view of the fact that significant cyber incidents will often involve at least the possibility of a nation-state actor or have some other national security nexus, the Department of Justice, acting through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, shall be the Federal lead agency for threat response activities.

b. The Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, shall be the Federal lead agency for asset response activities.

c. The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, shall be the Federal lead agency for intelligence support and related activities.

Drawing upon the resources and capabilities across the Federal Government, the Federal lead agencies are responsible for:

a. Coordinating any multi-agency threat or asset response activities to provide unity of effort, to include coordinating with any agency providing support to the incident, to include SSAs in recognition of their unique expertise;

b. Ensuring that their respective lines of effort are coordinated with other Cyber UCG participants and affected entities, as appropriate;

c. Identifying and recommending to the CRG, if elevation is required, any additional Federal Government resources or actions necessary to appropriately respond to and recover from the incident; and

d. Coordinating with affected entities on various aspects of threat, asset, and affected entity response activities through a Cyber UCG, as appropriate.

C. Field-Level Coordination

Field-level representatives of the Federal asset or threat response lead agencies shall ensure that they effectively coordinate their activities within their respective lines of effort with each other and the affected entity. Such representatives may be co-located with the affected entity.

VI. Unified Public Communications

The Departments of Homeland Security and Justice shall maintain and update as necessary a fact sheet outlining how private individuals and organizations can contact relevant Federal agencies about a cyber incident.

VII. Relationship to Existing Policy

Nothing in this directive alters, supersedes, or limits the authorities of Federal agencies to carry out their functions and duties consistent with applicable legal authorities and other Presidential guidance and directives. This directive generally relies on and furthers the implementation of existing policies and explains how United States cyber incident response structures interact with those existing policies. In particular, this policy complements and builds upon PPD–8 on National Preparedness of March 30, 2011. By integrating cyber and traditional preparedness efforts, the Nation will be ready to manage incidents that include both cyber and physical effects.

BARACK OBAMA

NOTE: An original was not available for verification of the content of this directive.

Categories: Directives : U.S. cyber incident coordination :: Policy directive.

Subjects: Civil rights : Privacy; Defense and national security : Cybersecurity :: Cyber attacks; Defense and national security : Cybersecurity :: Strengthening efforts; Defense and national security : Intelligence; Homeland Security, Department of : Secretary; Intelligence, Office of the Director of National; Justice, Department of : Bureau of Investigation, Federal.

DCPD Number: DCPD201600495.