Annex for Presidential Policy Directive -- United States Cyber Incident Coordination

SUBJECT: Federal Government Coordination Architecture for Significant Cyber Incidents

I. Scope

This annex to PPD-41, United States Cyber Incident Coordination Policy, provides further details concerning the Federal Government coordination architecture for significant cyber incidents and prescribes certain implementation tasks.

II. Coordination Architecture

1. National Policy Coordination

The Cyber Response Group (CRG) shall be chaired by the Special Assistant to the President and Cybersecurity Coordinator (Chair), or an equivalent successor, and shall convene on a regular basis and as needed at the request of the Assistant to the President for Homeland Security and Counterterrorism and Deputy National Security Advisor. Federal departments and agencies, including relevant cyber centers, shall be invited to participate in the CRG, as appropriate, based on their respective roles, responsibilities, and expertise or in the circumstances of a given incident or grouping of incidents. CRG participants shall generally include senior representatives from the Departments of State, the Treasury, Defense (DOD), Justice (DOJ), Commerce, Energy, Homeland Security (DHS) and its National Protection and Programs Directorate, and the United States Secret Service, the Joint Chiefs of Staff, Office of the Director of National Intelligence, the Federal Bureau of Investigation, the National Cyber Investigative Joint Task Force, the Central Intelligence Agency, and the National Security Agency. The Federal Communications Commission shall be invited to participate should the Chair assess that its inclusion is warranted by the circumstances and to the extent the Commission determines such participation is consistent with its statutory authority and legal obligations.

The CRG shall:

1. Coordinate the development and implementation of the Federal Government's policies, strategies, and procedures for responding to significant cyber incidents;
2. Receive regular updates from the Federal cybersecurity centers and agencies on significant cyber incidents and measures being taken to resolve or respond to those incidents;
3. Resolve issues elevated to it by subordinate bodies as may be established, such as a Cyber Unified Coordination Group (UCG);
4. Collaborate with the Counterterrorism Security Group and Domestic Resilience Group when a cross-

disciplinary response to a significant cyber incident is required;
5. Identify and consider options for responding to significant cyber incidents, and make recommendations to the Deputies Committee, where higher-level guidance is required, in accordance with PPD-1 on Organization of the National Security Council System of February 13, 2009, or any successor; and
6. Consider the policy implications for public messaging in response to significant cyber incidents, and coordinate a communications strategy, as necessary, regarding a significant cyber incident.

2. National Operational Coordination

To promote unity of effort in response to a significant cyber incident, a Cyber UCG shall:

1. Coordinate the cyber incident response in a manner consistent with the principles described in section III of this directive;
2. Ensure all appropriate Federal agencies, including sector-specific agencies (SSAs), are incorporated into the incident response;
3. Coordinate the development and execution of response and recovery tasks, priorities, and planning efforts, including international and cross-sector outreach, necessary to respond appropriately to the incident and to speed recovery;
4. Facilitate the rapid and appropriate sharing of information and intelligence among Cyber UCG participants on the incident response and recovery activities;
5. Coordinate consistent, accurate, and appropriate communications regarding the incident to affected parties and stakeholders, including the public as appropriate; and
6. For incidents that include cyber and physical effects, form a combined UCG with the lead Federal agency or with any UCG established to manage the physical effects of the incident under the National Response Framework developed pursuant to PPD-8 on National Preparedness.

SSAs shall be members of the UCG for significant cyber incidents that affect or are likely to affect their respective sectors. As set forth in Presidential Policy Directive 21, the SSAs for critical infrastructure sectors are as follows: DHS (Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Emergency Services, Government Facilities, Information Technology, Nuclear Reactors, Materials, and Waste, and Transportation Systems); DOD (Defense Industrial Base); Department of Energy (Energy); Department of the Treasury (Financial Services); Department of Agriculture (Food and Agriculture); Department of Health and Human Services (Healthcare and Public Health, and Food and Agriculture); General Services Administration (Government Facilities); Department of Transportation (Transportation Systems); and the Environmental Protection Agency (Water and Wastewater Systems).

A Cyber UCG shall operate in a manner that is consistent with the need to protect intelligence and law enforcement sources, methods, operations, and investigations, the privacy of individuals, and sensitive private sector information.

A Cyber UCG shall dissolve when enhanced coordination procedures for threat and asset response are no longer required or the authorities, capabilities, or resources of more than one Federal agency are no longer required to manage the remaining facets of the Federal response to an incident.

III. Federal Government Response to Incidents Affecting Federal Networks

Nothing in this directive alters an agency's obligations to comply with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA) or Office of Management and Budget (OMB) guidelines related to responding to an "incident," "breach," or "major incident" as defined in that statute and OMB guidance. Federal agencies shall follow OMB guidance to determine whether an incident is considered a "major incident" pursuant to FISMA. If the cyber incident meets the threshold for a "major incident," it is also a "significant cyber incident" for purposes of this directive and shall be managed in accordance with this directive.

1. Civilian Federal Networks

The Director of OMB oversees Federal agency information security policies and practices. The Secretary of Homeland Security, in consultation with the Director of OMB, administers the implementation of Federal agency information security policies and practices and operates the Federal information security incident center. The National Institute of Standards and Technology (NIST) develops standards and guidelines for Federal information systems that are mandatory for Federal agencies to implement.

Federal agencies shall respond to significant cyber incidents in accordance with this directive and applicable policies and procedures, including the reporting of incidents to DHS as required by the U.S. Computer Emergency Readiness Team Federal incident notification guidelines.

Where the effects of a significant cyber incident are limited to the operational activities of an individual Federal agency, that affected agency shall maintain primary authority over the affected assets and be responsible for managing the restoration services and related networks, systems, and applications and making the decision to restart an affected system. DHS and other Federal agencies shall provide support as appropriate.

Where a significant cyber incident has an impact on multiple Federal agencies or on the integrity, confidentiality, or availability of services to the public, the decision to restart an affected system rests with the owning Federal agency, but OMB and the Federal lead agencies for threat and asset response shall provide a consolidated, timely written recommendation, with appropriate caveats and conditions, to help inform that owning agency's decision.

2. DOD Information Network

The Secretary of Defense shall be responsible for managing the threat and asset response to cyber incidents affecting the Department of Defense Information Network, including restoration activities, with support from other Federal agencies as appropriate.

3. Intelligence Community Networks

The Director of National Intelligence shall be responsible for managing the threat and asset response for the integrated defense of the Intelligence Community (IC) information environment through the Intelligence Community Security Coordination Center, in conjunction with IC mission partners and with support from other Federal agencies, as appropriate.

IV. Implementation and Assessment

Federal agencies shall take the following actions to implement this directive:

1. Charter

Within 90 days of the date of this directive, the National Security Council (NSC) staff shall update the CRG charter to account for and support the policy set forth herein, which shall be submitted to the President through the Assistant to the President for Homeland Security and Counterterrorism.

2. Enhanced Coordination Procedures

Each Federal agency that regularly participates in the CRG, including SSAs, shall ensure that it has the standing capacity to execute its role in cyber incident response. To prepare for situations in which the demands of a significant cyber incident exceed its standing capacity, each such agency shall, within 90 days of the date of this directive, establish enhanced coordination procedures that, when activated, bring dedicated leadership, supporting personnel, facilities (physical and communications), and internal processes enabling it to manage a significant cyber incident under demands that would exceed its capacity to coordinate under normal operating conditions.

Within 90 days of the date of this directive, the SSAs shall develop or update sector-specific procedures, as needed and in consultation with the sector(s), for enhanced coordination to support response to a significant cyber incident, consistent with this directive.

Enhanced coordination procedures shall identify the appropriate pathways for communicating with other Federal agencies during a significant cyber incident, including the relevant agency points-of-contact, and for notifying the CRG that enhanced coordination procedures were activated or initiated; highlight internal communications and decisionmaking processes that are consistent with effective incident coordination; and outline processes for maintaining these procedures.

In addition, each Federal agency's enhanced coordination procedures shall identify the agency's processes and existing capabilities to coordinate cyber incident response activities in a manner consistent with this directive. The procedures shall identify a trained senior executive to oversee that agency's participation in a Cyber UCG. SSAs shall have a trained senior executive for each of the sectors for which it is the designated SSA under Presidential Policy Directive 21.

Within 120 days of the date of this directive, the SSAs shall coordinate with critical infrastructure owners and operators to synchronize sector-specific planning consistent with this directive.

3. Training

Within 150 days of the date of this directive, the Federal Emergency Management Agency shall make necessary updates to its existing Unified Coordination training to incorporate the tenets of this directive.

Within 150 days of the date of this directive, Federal agencies shall update cyber incident coordination training to incorporate the tenets of this directive.

Federal agencies shall identify and maintain a cadre of personnel qualified and trained in the National Incident Management System and Unified Coordination to manage and respond to a significant cyber incident. These personnel will provide necessary expertise to support tasking and decisionmaking by a Cyber UCG.

4. Exercises

Within 180 days of the date of this directive, Federal agencies shall incorporate the tenets of this policy in cyber incident response exercises. This will include exercises conducted as part of the National Exercise Program. Exercises shall be conducted at a frequency necessary to ensure Federal agencies are prepared to execute the plans and procedures called for under this directive. When appropriate, exercises shall consider the effectiveness of the end-to-end information sharing process.

5. Cyber UCG Post-Incident Review

Upon dissolution of each Cyber UCG, the Chair of the CRG shall direct a review of a Cyber UCG's response to a significant cyber incident at issue and the preparation of a report based on that review to be provided to the CRG within 30 days. Federal agencies shall modify any plans or procedures for which they are responsible under this directive as appropriate or necessary in light of that report.

6. National Cyber Incident Response Plan

Within 180 days of the date of this directive, DHS and DOJ, in coordination with the SSAs, shall submit a concept of operations for the Cyber UCG to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Director of OMB, that is consistent with the principles, policies, and coordination architecture set forth in this directive. This concept of operations shall further develop how the Cyber UCG and field elements of the Federal coordination architecture will work in practice for significant cyber incidents, including mechanisms for coordinating with Federal agencies managing the physical effects of an incident that has both cyber and physical elements and for integration of private sector entities in response activities when appropriate. The Secretary of Homeland Security shall, as appropriate, incorporate or reference this concept of operations in the Cyber Incident Annex required by section 205 of the Cybersecurity Act of 2015.

Within 180 days of the date of this directive, the Secretary of Homeland Security, in coordination with the Attorney General, the Secretary of Defense, and the SSAs, shall submit a national cyber incident response plan to address cybersecurity risks to critical infrastructure to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Director of OMB, that is consistent with the principles, policies, and coordination architecture set forth in this directive. The Secretary of Homeland Security shall ensure that the plan satisfies section 7 of the National Cybersecurity Protection Act of 2014. This plan shall be developed in consultation with SLTT governments, sector coordinating councils, information sharing and analysis organizations, owners and operators of critical infrastructure, and other appropriate entities and individuals. The plan shall take into account how these stakeholders will coordinate with Federal agencies to mitigate, respond to, and recover from cyber incidents affecting critical infrastructure.

Share This: