The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

**MEMO# 30133**

August 15, 2016

# President Issues Policy Directive on United States Cyber Incident Coordination

[30133]

August 15, 2016

TO: TECHNOLOGY COMMITTEE No. 12-16
CHIEF INFORMATION SECURITY OFFICER ADVISORY COMMITTEE RE: PRESIDENT ISSUES POLICY DIRECTIVE ON UNITED STATES CYBER INCIDENT COORDINATION

On July 26th, the White House published Presidential Policy Directive No. 41 ("PPD") on the subject of United States Cyber Incident Coordination. [1] While the PPD notes that "United States preparedness efforts have positioned the Nation to manage a broad range of threats and hazards effectively," it acknowledges that "certain cyber incidents that have significant impacts on an entity, our national security, or the broader economy require a unique approach to response efforts." The PPD sets forth principles governing the Federal Government's response to any cyber incident – involving government or private sector entities – and establishes lead Federal agencies and an architecture for coordinating the government's response to such incident. Following a "Scope" and "Definitions" section, the PPD consists of five substantive sections, each of which is briefly summarized below.

## I. Principles Guiding Incident Response

This section discusses: (a) the "Shared Responsibility" between individuals, the private sector, and government agencies in protecting the nation from malicious cyber activity and managing cyber incidents; (b) the "Risk-Based Response" that the Federal Government will use to determine its response actions and the resources it will deploy in responding; (c) the Federal Government "Respecting affected entities" by safeguarding non-public details of an incident and sensitive private sector information to the extent permitted by law; (d) the "Unity of Governmental Efforts" that will occur to ensure that efforts of governmental agencies are coordinated to achieve optimal results; and (e) "Enabling Restoration and Recovery" to ensure that Federal response activities are conducted in a manner to facilitate both restoration and recovery of an entity that has experienced a cyber incident and balance investigative and national security requirements, public health and safety, and the need to return to normal operations as quickly as possible.

## II. Concurrent Lines of Effort

This section of the PPD states that, 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. Additionally, if a Federal agency is an affected entity, it shall undertake a fourth concurrent line of effort." [2] The PPD summarizes what each of these concurrent lines of effort consists of. With respect to the “Asset Response activities, the PPD states that these 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. [3]

## III. Architecture of Federal Government Response Coordination for Significant Cyber Incidents

According to this section of the PPD, the Federal Government will coordinate its activities in three ways. The first is through a “National Policy Coordination” in which the Cyber Response Group (CRG), in support of the National Security Council (NSC) Deputies and Principals Committee shall coordinate the development and implementation of the United States’ policy and strategy to “significant” cyber incidents affecting the United States or its interests abroad. [4]

The second means of coordination is through “National Operational Coordination.” This section of the PPD requires “Agency Enhanced Coordination Procedures,” which involve each Federal agency that regularly participates in the CRG (including relevant sector specific agencies) [5] to establish and follow enhanced coordination procedures for situations in which the demands of responding to a significant cyber incident exceed the agency’s standing capacity. In addition to the responsibilities imposed on each agency, a Cyber United Coordination Group shall coordinate between and among Federal agencies on the agencies’ response efforts and will integrate private sector partners into incident response efforts “as appropriate.” [6] The PPD also assigns the following agencies the following leads: the Department of Justice, acting through the FBI and the National Cyber Investigative Task Force, shall be the Federal lead agency for threat response activities; the Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, shall be the lead agency for asset response activities; and the Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, shall be the lead agency for intelligence support and related activities.

The third means of coordination is “Field-Level,” in which 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.” [7]

## IV. Unified Public Communications

This section of the PPD requires the Departments of Homeland Security and Justice to maintain and update as necessary a “fact sheet outlining how private individuals and

organizations can contact relevant Federal agencies about a cyber incident." [8]

## V. Relationship to Existing Policy

This section of the PPD affirms that nothing in the PPD alters, superseded, or limits the authorities of Federal agencies to carry out their functions and duties consistent with their legal authority. It additionally notes that this PPD "complements and builds upon PPD-8 on National Preparedness" and that by "integrating cyber and traditional preparedness efforts, the Nation will be ready to manage incidents that include both cyber and physical effects." [9]

Tamara K. Salmon
Associate General Counsel

**endnotes**

[1] See Presidential Policy Directive – United States Cyber Incident Coordination, PPD-41, The White House (July 26, 2016), which is available at: https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[2] PPD at p. 4.

[3] PPD at p. 5.

[4] The PPD notes that the CRG is "accountable through the Assistant to the President for Homeland Security and Counterterrorism to the NSC chaired by the President." PPD at p. 6.

[5] It does not appear that the SEC participates in the CRG, nor is it considered a "sector specific agency." Instead, according to the Department of Homeland Security, the Department of the Treasury is the sector-specific agency for the financial services sector. The other agencies that are sector specific agencies are the Departments of Defense, Energy, Agriculture, Health and Human Services, and Transportation, as well as the General Services Administration and the Environmental Protection Agency. A list of the United States' 16 critical infrastructure sectors and the agencies responsible for them is available at: https://www.dhs.gov/sector-specific-agencies.

[6] PPD at p. 6. This section of the PPD discusses in more detail the logistics associated with this coordination activity.

[7] PPD at p. 8.

[8] Id.

[9] PPD at p. 9. PPD-8 is available at: https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.