CLIENT ALERT

Presidential Policy Directive Lays Groundwork for National Incident Response Plan

Jul.28.2016

On Tuesday, President Obama approved a new Presidential Policy Directive (PPD) on "United States Cyber Incident Coordination" that establishes a path for how the government will identify and respond to "significant" cyber incidents, including which federal agencies will lead such efforts and how they will coordinate across the public and private sectors. Stemming from the Cybersecurity National Action Plan, the PPD does not expand current legal requirements, but it does represent a first step towards developing a robust federal cybersecurity response plan with significant input from the private sector.

Embracing the need to create a unified effort within the government and coordination between the public and private sectors, the PPD sets forth five guiding principles for incident response: (1) sharing responsibility between the private sector and government agencies; (2) adopting a risk-based approach to government response; (3) respecting the need for confidentiality by entities affected by cyber incidents; (4) unifying government efforts in coordinating roles and responsibilities; and (5) enabling restoration and recovery for entities affected by cyber incidents.

Consistent with the approach advocated by many companies in the private sector, the PPD also incorporates the government's risk-based, six-level "severity schema" to provide a common framework for describing cyber incidents. Level 0 is the baseline. Cyber incidents at Level 3 and above are considered "significant" cyber incidents that are the primary focus of the PPD and that merit a unified response. "Significant" cyber incidents include those that are "likely to result in a demonstrable impact" (Level 3) or "likely to result in a significant impact" (Level 4) to "public health or safety, national security, economic security, foreign relations, or civil liberties." Level 5 is an emergency status reserved for cyber incidents that "pose an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons."

The PPD further establishes three concurrent "lines of effort" for federal agencies and identifies which agencies are responsible for each:

Line of Effort	Responsible Agency
Threat Response	Federal Bureau of Investigation (FBI)
Asset Response	Department of Homeland Security (DHS)
Intelligence Support	Office of the Director of National Intelligence (ODNI)

Additionally, the PPD establishes three ways in which the government will coordinate its response activities for significant cyber incidents—national policy coordination, national operational coordination, and field-level coordination. Most notably, the Cyber Unified Coordination Group (UCG) will serve as the primary method for coordinating federal agencies. The UCG normally consists of federal lead agencies for threat response, asset response, and intelligence support, but depending on the scope,

nature, and facts of a particular significant cyber incident, a Cyber UCG may include participation from other agencies or even the private sector.

Although the PPD explains that, while the government "typically will not play a role" in managing the impact of a cyber incident when the affected entity is solely from the private sector, the relevant sector-specific agency (SSA) is tasked with coordinating government efforts "to understand the potential business and operational impact of a cyber incident on private sector critical infrastructure." Under the PPD framework, the private sector now also has opportunities to coordinate with government stakeholders in the event of a significant cyber incident, including DHS, FBI and, if necessary, ODNI, with more certainty and definition based on the nature of the incident and the organization's background.

Moreover, the government is directed to consult with the private sector in developing a federal cybersecurity incident response plan. For example, DHS must, within 180 days, coordinate with the Attorney General, the Department of Defense, and SSAs to submit to the President "a national cyber incident response plan to address cybersecurity risks to critical infrastructure" that is consistent with the principles, policies, and coordination architecture set forth in the PPD. As part of this effort, DHS is required to consult with critical infrastructure owners and operators (as well as information sharing and analysis organizations, state and local governments, and sector coordinating councils) to determine how these stakeholders will "mitigate, respond to, and recover from cyber incidents affecting critical infrastructure." Because most of the critical energy infrastructure in the United States is privately owned, the new and increased role of the federal government in developing a national response plan is likely to have important implications for these companies.

In addition, within 90 days, the SSAs, including, for example, the Transportation Security Administration for the pipeline sector and the Department of Energy for the utility sector, must develop or update sector-specific procedures, "as needed and in consultation with the sector(s)," for an enhanced incident response plan. In this sense, the PPD is acknowledging the crucial role that the private sector plays in securing our nation's cybersecurity and the inevitable need for coordination between the government and private industry.

Notably missing from the PPD is any reference to the Cybersecurity Information Sharing Act of 2015 (CISA) and, therefore, any indication regarding how the liability and other protections offered by CISA will be preserved by the information sharing opportunities contemplated by the PPD including during the threat response and investigation phases when the PPD contemplates "facilitating information sharing and operational coordination with asset response." Also absent is any mention of the government's recent efforts to shore up the cybersecurity of its supply chain. Here, too, recent regulations have aimed at enhancing cybersecurity within the federal contracting community, including with respect to how cyber incidents are handled.

The release of the cyber Incident Coordination Directive is a first step towards a unified national response to cyber threats. Its implementation, however, will take many months and require a coordinated approach by the public and private sectors.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Maida Oringher Lerner
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2596
Email: mlerner@crowell.com

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Charles Baek
Counsel – Washington, D.C.
Phone: +1 202.624.2894
Email: cbaek@crowell.com