The White House has released a Presidential Policy Directive on United States Cyber Incident Coordination (PPD-41). PPD-41 is part of President Obama’s broader Cybersecurity National Action Plan, which was unveiled this past February.

PPD-41 is primarily geared toward “significant cyber incidents,” which are “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States” and require close coordination between the public and private sectors. The Directive first sets forth several principles to guide the federal government’s response to any cyber incident (defined to include both actual events and security vulnerabilities): shared responsibility, risk-based response, respecting affected entities, unity of government effort, and enabling restoration and recovery. It also directs federal agencies to undertake four “concurrent lines of effort” in responding to cyber incidents:

- Threat response, coordinated by the Federal Bureau of Investigation (FBI);
• Asset response, coordinated by the Department of Homeland Security (DHS);
• Intelligence support and related activities, coordinated by the Office of the Director of National Intelligence;
• For cyber incidents impacting federal agencies, managing the effects on the agencies’ operations, customers, and workforce.

With respect to significant cyber incidents, PPD-41 sets forth an architecture for the federal government’s coordination and incident response. First, the Directive calls for national policy coordination via the Cyber Response Group (CRG) to support the National Security Council in developing and implementing federal government policy and strategy with respect to significant cyber incidents. Second, the Directive calls for national operational coordination by each federal agency that regularly participates in the CRG, and a Cyber Unified Coordination Group to facilitate that coordination and integration of private sector partners into incident response where appropriate. Third, the Directive calls for field-level representatives of the FBI and DHS to ensure effective coordination of the response to significant cyber incidents. Additional details about the PPD-41 architecture are contained in an annex to the Directive.

Finally, PPD-41 directs DHS and the Department of Justice to maintain and update a fact sheet outlining how private entities can contact relevant federal agencies about cyber incidents. The FBI and DHS each released statements touting the release of PPD-41.

© 2021 Covington & Burling LLP

National Law Review, Volume VI, Number 210