CLIENT ALERT

President Issues Executive Order to Strengthen Cybersecurity of Federal Networks and U.S. Critical Infrastructure

May.12.2017

Yesterday, President Trump signed Executive Order 13228 entitled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The Order focuses on: (1) enhancing and harmonizing federal network protection; (2) redoubling protection of U.S. critical infrastructure; and (3) improving overall U.S. cybersecurity protection and capabilities. Notably, the Order mandates more than a dozen agency reports that will form the basis for the adoption of further substantive policies in these three areas.

Among other measures, the Order mandates that executive agencies use the National Institute of Standards and Technology (NIST) Cybersecurity Framework to manage their agency's cyber risk. While many agencies were already doing so, this is significant because it represents a clear endorsement by the new Administration of these important standards. The Order also requires the Department of Homeland Security to engage with owners and operators of the nation's critical infrastructure to identify how agencies can support cybersecurity efforts and report to the president within 180 days on findings and recommendations for better supporting critical infrastructure entities.

Specific Risk Areas

The Order singles out three primary areas for specific risk analysis: critical infrastructure at greatest risk (so-called "Section 9 Entities"); the core communications infrastructure; and the electric subsector.

Section 9 Entities

The Order instructs national security leadership to engage with critical infrastructure entities as defined in Section 9 of Executive Order 13636. (Crowell & Moring's summary of that executive order can be accessed here.) Section 9 entities are those organizations that control critical infrastructure in which "a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." During the process established by the Order, Section 9 entities will provide recommendations for how federal agencies can best support their cyber risk management efforts.

Communications Infrastructure

To secure U.S. critical communications networks, the Order mandates a report from agencies with recommendations to fortify the nation's core communications infrastructure. Specifically, the Order identifies the goal of reducing automated and distributed attacks (like "botnets"). Botnet attacks have, in recent years, become tools of choice for hackers to commit mass cyberattacks.

Electric Subsector

The Order instructs the Department of Energy and DHS to consult with other stakeholders supporting the electric grid to study the grid's readiness to respond to a significant cyber incident. Alarming attacks on power grids have occurred recently in other nations, and key security stakeholders in the U.S. have raised the alarm about the potential vulnerabilities of America's electric infrastructure to similar attacks.

Federal Networks

Importantly, the Order mandates that each federal agency immediately adopt the NIST Cybersecurity Framework to manage the agency's cybersecurity risk. Prior to this Order, the NIST Cybersecurity Framework had been highly influential, but not mandatory. Within 90 days, each agency head must provide the administration with an update on the agency's implementation of the Framework and identify any unmitigated vulnerabilities in their agency's cybersecurity infrastructure. In the Order, the president made clear that he will hold agency heads accountable for implementing risk-based measures to manage the cybersecurity of their organizations.

Notable also is the Order's emphasis on shared IT services. The Order requests an interagency study examining the feasibility of "transitioning all agencies to . . . Shared IT services, including email, cloud services, and cybersecurity services." It also directs agency heads to show preference in their government contracting for Shared IT services. These sweeping instructions could foreshadow a universal shift to Shared IT services, which has long been a cross-agency priority for the federal government.

Potential Opportunities to Comment

The Order requires multiple agencies to conduct in-depth risk analyses and to issue reports with recommendations for improving the nation's cybersecurity capabilities. Many of these analysis windows may provide interested stakeholders with an opportunity to provide input.

Reports due within 90 days of the Order:

- **Electric subsector companies** may submit opinions to DHS and DOE about gap analysis and response readiness relating to potential significant cyber incidents.
- **Section 9 entities (especially publicly-traded Section 9 entities)** may provide comments to DHS and the Commerce Department about the adequacy of current federal policies to promote market transparency of cyber risk management practices.
- **Defense Contractors** might be consulted on cybersecurity risks impacting the Defense Industrial Base's supply chain. A multiagency team will study this issue, including the DHS, DoD, FBI, and the Director of National Intelligence (DNI).
- **Any entity using networked technology** might participate in providing opinions about the best strategies to combat illicit uses of that networked technology.

Reports due within 180 days of the Order:

- **Section 9 entities** may submit recommendations for how federal agencies could better use their cybersecurity authorities and capabilities to support critical infrastructure cybersecurity. Multiple agencies will be involved in this dialogue, including DoD, DHS, FBI, the DNI, and the Attorney General.

Reports due within 240 days of the Order:

- **Core communications companies** may submit recommendations to DHS and the Commerce Department relating to improving the communications network's resilience and reducing the risk of automated and distributed attacks.

The Order and the reports and consultations it mandates are expected to be the harbingers of numerous additional actions that the Trump Administration will take to help counter the nation's growing cyber threats and to protect its digital infrastructure, while reflecting an appreciation for the role that private industry will play in this effort.

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

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

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

Peter B. Miller, CIPP/G/US/E, CIPM, CIPT
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2506
Email: pmiller@crowell.com

Justin Kingsolver
Associate – Washington, D.C.
Phone: +1 202.624.2927
Email: jkingsolver@crowell.com