Privacy and Information Governance

New Cybersecurity Executive Order Affects Critical Infrastructure Industry Sectors, Including Communications, Electricity and Defense

By: Nancy Libin, Cindy Robertson and Andrew D. Irwin

On May 11, 2017, President Trump signed a long-awaited Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (the "Executive Order"), which directs federal government agencies to take certain steps to strengthen the cybersecurity of both federal networks and critical infrastructure. The Executive Order builds on previous Obama-era executive orders and presidential policy directives regarding the cybersecurity of both public and private sector networks.

With respect to the private sector, the Executive Order focuses on critical infrastructure, and in particular, on companies in the communications and electric industries, and the defense industrial base. In addition to directing the Secretaries of the Departments of Homeland Security ("DHS"), Commerce ("Commerce"), Energy ("Energy"), and Defense ("Defense") to conduct reviews and provide reports to the President regarding the sufficiency of certain federal and private sector cybersecurity authorities and practices, the Executive Order appears to provide industry participants with an opportunity to engage with federal agencies as they conduct reviews and make findings and recommendations to the President. Moreover, the Executive Order also may create new business opportunities for government contractors that provide cloud and cybersecurity services, and it could result in new regulatory standards for defense contractors.

We provide highlights of the Executive Order below.

I. Action to Protect the Cybersecurity of Critical Infrastructure

The Executive Order states that it is the policy of the executive branch to "use its authorities and capabilities to support the cybersecurity risk management of the owners and operators of the Nation's critical infrastructure."[1]

Critical Infrastructure "At Greatest Risk"

The Secretary of DHS, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the FBI, and the heads of sector-specific agencies (as defined in Presidential Policy Directive 21[2]), must (a) identify "authorities and capabilities" that agencies could use "to support the cybersecurity efforts" of companies that DHS has determined are "at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security,"[3] (b) engage those entities and solicit their input regarding how the "authorities and capabilities" identified could be used, and (c) provide a report regarding the same to the President within 6 months.

Companies in the Communications and Internet Sectors

The Secretaries of DHS and Commerce must lead an "open and transparent process" to "identify and promote action" by "appropriate stakeholders" to "improve the resilience of the internet and communications ecosystem" and to "encourage collaboration" with the "goal of dramatically reducing threats perpetrated by automated and distributed attacks."[4] The Executive Order directs the Secretaries of DHS and Commerce "to consult with" the Secretary of Defense, the Attorney General, the

Director of the FBI, the chairs of the FCC and FTC, the heads of sector-specific agencies, and "appropriate stakeholders," defined as "any non-executive branch person or entity that elects to participate," during this process. Therefore, assuming that "appropriate stakeholders" include representatives from relevant companies, there may be an opportunity for interested industry participants to engage and influence government representatives as the government identifies "action" necessary to reduce cybersecurity threats in the communications and internet sectors.

Companies that Provide Electricity or Support the Electric Grid

The Executive Order likewise directs the Secretaries of Energy and DHS to consult with the Office of the Director of National Intelligence; State, local, tribal, and territorial governments; and "with others as appropriate," to assess (a) the "potential scope and duration of a prolonged power outage associated with a significant cyber incident," (b) the "readiness of the United States to manage the consequences" of such an incident, and (c) any "gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident."[5] The Executive Order directs Energy and DHS to consult "others as appropriate," rather than "appropriate stakeholders," but this section, too, may provide an opportunity for interested companies in this sector to participate in this assessment.

Defense Industrial Base

The Executive Order requires the Secretaries of DOD and DHS, with the Directors of the FBI and National Intelligence, to provide a report within 90 days on "cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities."[6] This report must recommend methods for mitigating these defense-related cyber risks. Another report, due 150 days from the Executive Order, issued by the same agency heads and the Secretary of Commerce, will address the "scope and sufficiency" of U.S. efforts to "ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities."[7] Depending on the outcome of both reports, defense contractors may well become subject to more rigorous regulatory standards. At a minimum, contractors could receive more clarity on the extent to which they are required to ensure their supply chain meets appropriate standards.

II. Action to Protect Federal Networks and Data

The Executive Order also addresses the protection of federal information technology and data. It expressly makes heads of federal agencies and departments responsible for managing cybersecurity risks in their respective agencies,[8] and it directs them to both implement the National Institute for Standards and Technology ("NIST") cybersecurity framework ("NIST Framework"), and submit, within 90 days, a risk management report to the Secretary of DHS and the Director of the Office of Management and Budget ("OMB"), detailing the agency's "risk mitigation and acceptance choices" and plan for implementing the NIST Framework in their respective agencies.[9]

In addition, because the Executive Order directs heads of agencies to "show preference in their procurement for shared IT services," the Order also may boost government contractors that provide cloud services to government agencies. (This requirement also continues policy implemented by the Obama administration with respect to migration to shared IT services.[10])

III. Next Steps

Companies in relevant industry sectors should be alert for information regarding how to participate in these processes. Notably, companies may elect to engage not only with federal agencies directly, but also with NIST, which recently released a new draft of "The Cybersecurity Framework: Implementation Guidance for Federal Agencies" (NISTIR 8170). NIST states that public feedback, due by June 30, will help "to determine which Cybersecurity Framework concepts are incorporated into future versions of the suite of NIST security and privacy risk management publications." Cybersecurity companies should likewise note the emphasis within the Executive Order to "address immediate unmet budgetary needs necessary to manage risk to the executive branch enterprise,"[11] foretelling of future administrative

pressure on Congress to provide adequate funding for the Executive Order's cybersecurity directives and agency recommendations.

---

[1] Executive Order, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* May 11, 2017 ("Executive Order"), Section 2(a).

[2] Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, Feb. 12, 2013.

[3] These are critical infrastructure entities identified pursuant to Section 9 of Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, Feb. 12, 2013. See the Jenner & Block analysis of this Executive Order here.

[4] Executive Order, Section 2(d).

[5] Executive Order, Section 2(e).

[6] Executive Order, Section 2(f).

[7] Executive Order, Section 3(d)(iii).

[8] Executive Order, Section 1(a).

[9] Executive Order, Section 1(c).

[10] *See* Executive Office of the President, *Federal Information Technology Shared Services Strategy*, May 2, 2012, https://cio.gov/wp-content/uploads/downloads/2012/09/Shared_Services_Strategy.pdf.

[11] Executive Order, Section 1(c)(iv)(B)(2).

Contact Us

Nancy C. Libin
nlibin@jenner.com | Download V-Card

Cynthia J. Robertson
crobertson@jenner.com | Download V-Card

Andrew D. Irwin
airwin@jenner.com | Download V-Card