Skadden

PRIVACY & CYBERSECURITY UPDATE

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES

02.13.13

President Issues Cybersecurity Executive Order

On February 12, 2013, President Obama signed both an executive order[1] and a presidential directive[2] that together set forth the administration's approach to two key cybersecurity-related issues: (i) regulating critical infrastructure network security, and (ii) sharing cyber threat information between the public and private sectors. Together, the order and the directive represent a White House response to the congressional deadlock on cybersecurity legislation. While members of both parties have suggested that action on cybersecurity is a priority, separate bills advanced in the House and Senate in the last Congress have not yet been reconciled. While both the House and Senate bills contemplated new safeguards and exceptions to existing data privacy laws for businesses that share cybersecurity threat information with the government, both did so on different terms.[3] In addition, the Senate bill asked the Department of Homeland Security (DHS) and regulatory agencies to work together to craft network security regulations that would be applied to critical private-sector infrastructure operators, while the House bill declined to add any new regulatory provisions. Conflicts over these different approaches have stalled legislative action and now have led the White House to issue the order and the directive to address the open issue. While further legislative action remains a possibility, national security and regulatory agencies have new marching orders in the interim.

The executive order discusses the cybersecurity of "critical infrastructure" — private sector systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, the economy or public health.[4] This definition has been imported from the USA PATRIOT Act[5] and has previously been interpreted broadly in Homeland Security Presidential Directive 7 (HSPD-7) to include entities such as financial services providers, energy companies and health care providers.[6] The presidential directive accompanying the executive order replaces HSPD-7 and broadens the set of critical infrastructure sectors even further, defining the new list to include:

- chemical;
- critical manufacturing;
- dams;
- defense industrial base;
- emergency services,
- energy;
- financial services;
- food and agriculture;

---

1 The White House — Office of the Press Secretary, *Executive Order: Improving Critical Infrastructure Cybersecurity*, Feb. 12, 2013 (Cybersecurity Executive Order).

2 *Presidential Policy Directive PPD-21: Critical Infrastructure Security and Resilience*, Feb. 12, 2013 (PPD-21).

3 *See* Cybersecurity Act of 2012, S.3414; Cyber Intelligence Sharing and Protection Act, H.R. 3523.

4 Cybersecurity Executive Order § 2.

5 *Compare* Cybersecurity Executive Order § 2 *with* 42 U.S.C. § 5195c(e) (both using an identical definition).

6 HSPD-7, http://www.dhs.gov/homeland-security-presidential-directive-7.

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or your regular Skadden contact.

Stuart D. Levi
New York Office
T: 212.735.2750
stuart.levi@skadden.com

Antoinette C. Bush
Washington, D.C.
202.371.7230
antoinette.bush@skadden.com

Ivan A. Schlager
Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

John M. Beahn
Washington, D.C.
202.371.7392
john.beahn@skadden.com

Joshua F. Gruenspecht
Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

Four Times Square
New York, NY 10036
Telephone: 212.735.3000

1440 New York Avenue, NW
Washington, D.C. 20005
Telephone: 202.371.7000

WWW.SKADDEN.COM

- government facilities;
- health care and public health;
- information technology;
- nuclear services;
- transportation systems; and
- water systems.[7]

The sectors most likely to see new regulation include energy (including the electric grid, natural gas and nuclear energy providers), defense contracting, transportation and information technology. However, companies in any of the targeted industries listed above should be aware of potential new obligations and opportunities arising out of the executive order, as detailed below.

Regulating Critical Infrastructure

The executive order initiates a new process through which federal agencies are asked to assess the need for new regulation of cybersecurity standards at critical infrastructure companies. There are three key components of this process: actions taken by the DHS, actions taken by the National Institute of Standards and Technology (NIST), and actions taken by sector-specific regulators named in the associated presidential directive (the Sector-Specific Agencies).

The specific set of entities potentially subject to new cybersecurity regulation will be determined by DHS, which is the lead agency for the new executive branch initiative.[8] DHS has 150 days after the issuance of the order to identify subgroups of critical infrastructure operators on whose networks a cybersecurity incident could result in "catastrophic regional or national effects on public health or safety, economic security, or national security."[9] Owners of identified critical infrastructure will be confidentially notified of that designation by DHS and given an opportunity to request reconsideration.[10] Notably, commercial information technology products and consumer information technology services are explicitly excluded from categorization as identified critical infrastructure.[11] This carve-out, the result of White House discussions with the technology industry early in the drafting process,[12] will limit the applicability of the more coercive portions of the executive order to providers of cloud services and consumer software.

At the same time, the executive order also orders NIST to coordinate the development of a framework to reduce cybersecurity risks to critical infrastructure (the Cybersecurity Framework).[13] The Cybersecurity Framework is intended to be technology-neutral, to apply across all critical infrastructure sectors and to include information security measures and controls.[14] NIST also is ordered to engage in an open public review and comment process as part of the drafting process.[15] A preliminary version of the Cybersecurity Framework is expected within 240 days after the issuance of the order and a final version within a year.[16] DHS is ordered to coordinate the development of a set of incentives to encourage the voluntary adoption of the Cybersecurity Framework by the private sector.[17]

Once the preliminary Cybersecurity Framework is published, the executive order asks each Sector-Specific Agency to assess its regulatory authorities and submit a report within 90 days to the White House and the Office of Management and Budget stating "whether or not the agency has clear authority to establish requirements based upon the [NIST framework]

---

7 *PPD-21*, section entitled "Designated Critical Infrastructure Sectors and Sector-Specific Agencies."

8 *PPD-21*, section entitled "Roles and Responsibilities."

9 Cybersecurity Executive Order § 9(a).

10 Cybersecurity Executive Order § 9(c).

11 Cybersecurity Executive Order § 9(a).

12 *See* Declan McCullagh, *Obama Signs Long-Awaited Cybersecurity Executive Order*, CNET, Feb. 12, 2013.

13 Cybersecurity Executive Order § 7(a).

14 Cybersecurity Executive Order § 7(b).

15 Cybersecurity Executive Order § 7(d).

16 Cybersecurity Executive Order § 7(e).

17 Cybersecurity Executive Order § 8.

to sufficiently address current and projected risks to critical infrastructures,"[18] with specific consideration of DHS-identified critical infrastructures.[19] If existing requirements are insufficient, the Sector-Specific Agencies are told to propose "actions" to mitigate cyber risk within 90 days of the publication of the final Cybersecurity Framework.

Companies identified as critical infrastructure can expect these actions to include new regulation where existing cybersecurity regulation is deemed insufficient. **However, given the multiple layers of administrative process involved in the establishment of any new cybersecurity regulations, and the emphasis placed in the executive order on consultation with the private sector as part of the implementation of any new regulatory regime, in-house counsel may want to consider providing input into the regulatory process in order to shape prospective new regulatory regimes.**[20] Skadden Arps can assist companies that wish to avail themselves of opportunities to provide formal comment or participate informally in sector-specific public-private information-sharing bodies.

Cybersecurity-Related Information Sharing Between Private Operators and Federal Agencies

Separately, the executive order asks DHS, the Department of Justice and the Office of the Director of National Intelligence to take measures to rapidly declassify and disseminate cybersecurity threat information.[21] In addition, the executive order asks DHS and the Department of Defense to expand the accessibility of the Enhanced Cybersecurity Services program — under which the government shares classified cyber threat information with private companies in order to assist them in defending their networks — to all critical infrastructure sectors.[22]

In-house counsel engaged in assessing risks, reviewing network security and developing policies to address cybersecurity concerns should consider this a potential opportunity to acquire more information on the network threat environment. Skadden Arps can provide insight on the benefits and limitations associated with participation in such programs.

Skadden practice groups with experience in various aspects of cybersecurity include Privacy and Data Security, Communications and CFIUS/National Security, which work with other components of our transactional, litigation and regulatory practices as appropriate.

---

18 Cybersecurity Executive Order § 10(a).

19 *Id.*

20 Note that the order is restricted in its application to agencies that are not "independent regulatory agencies." *See* 44 U.S.C. § 3502(5) for a list of independent regulatory agencies. Because certain companies in critical infrastructure sectors are normally regulated by independent agencies, those companies may find themselves subject to regulation in this specific area by government agencies with whom they otherwise do not have significant contacts.

21 Cybersecurity Executive Order §§ 4(a), 4(b).

22 Cybersecurity Executive Order § 4(c).