WILMERHALE

President Obama Issues Cybersecurity Executive Order

2013-02-13

President Obama yesterday signed an Executive Order aimed at improving the cybersecurity of the country's critical infrastructure ("CI").[1] The Order: (i) directs the National Institute of Standards and Technology ("NIST"), through a consultative process with other agencies and CI owners and operators, to develop cybersecurity performance standards and methods to reduce risks to CI ("Cybersecurity Framework"); (ii) directs the Department of Homeland Security ("DHS") and agencies responsible for CI sectors to create a program to encourage CI owners and operators to voluntarily adopt the Cybersecurity Framework established by NIST; (iii) directs agencies that have statutory authority to regulate CI to determine whether they have "clear authority" to establish mandatory standards based on the Cybersecurity Framework and, if current regulatory requirements are deemed insufficient, to impose such standards through rulemaking; (iv) expands to all CI sectors a government cybersecurity program that started at the Department of Defense ("DoD") for companies that are members the Defense Industrial Base ("DIB") and requires key federal agencies to provide more cybersecurity threat information to CI owners; (v) instructs the General Services Administration ("GSA") and DoD to look into incorporating cybersecurity standards into federal acquisition and procurement policies; and (vi) requires an annual report to the President about the extent to which CI owners and operators are participating in the voluntary program.

The Executive Order is significant for a number of reasons, including:

- There will likely be pressure on CI owners and operators to adopt the new voluntary cybersecurity standards created by NIST.
- A number of sector-specific agencies may propose additional mandatory cybersecurity regulations based on the NIST standards within a year or so. Among the sectors mostly likely to see new mandatory regulations may be the electric grid, natural gas, transportation, chemicals, nuclear power, and ports because agencies in those sectors appear to have existing statutory authority and industry standards are viewed by some as not being strong enough.
- Government contractors may also face new cybersecurity mandates. The specific mention in the Executive Order of incorporating security standards into acquisition planning makes it likely that the Federal Acquisition Regulations ("FAR") will be amended to include a cybersecurity procurement preference in future government contracts, a change also

supported by the government's considerable statutory authority to regulate contractors under the Federal Information Security Management Act, 44 U.S.C. § 3541 et seq. As with other government contracting requirements, that could open new avenues for potential False Claims Act liability.

- The Order will result in an expansion of opportunities for CI owners and operators to receive cybersecurity threat information (including classified information) from the government. Existing public-private cybersecurity programs available only to DIB companies may now be available to CI owners and operators who want to participate and can meet applicable security and legal requirements.
- The inclusion of IT companies of various kinds in additional cybersecurity standards is unclear. On the one hand, the Order prohibits DHS from identifying any "commercial information technology products or consumer information technology services" as CI at greatest risk, and sector-specific agencies are directed to "consider" the DHS CI-at-greatest-risk determinations in deciding whether to propose new cybersecurity regulations. That may mean that products and services satisfying that definition will not be the subject of new sector-specific requirements. On the other hand, the basic definition of CI itself does not include an express exemption for products and services used by CI.
- As new cybersecurity standards are established pursuant to the Order, public companies should evaluate whether their current disclosures in periodic reports filed with the Securities and Exchange Commission ("SEC") need to be updated in accordance with both disclosure guidance issued by SEC in October 2011 and general disclosure standards. For example, a public company may need to provide additional disclosure regarding material expenditures anticipated in connection with regulatory compliance or voluntary adoption of new standards, as well as any materially higher business risks associated with cybersecurity or government contracts identified as a result of the Order.[2]

Section-by-Section Analysis

Section 1: Policy: States that the policy of the United States is to "enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" through partnerships with CI owners and operators.

Section 2: Critical Infrastructure Definition: Defines CI, as already defined in statute at 42 U.S.C. § 5195c(e), as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Section 3: Policy Coordination: Provides the National Security Council with overall responsibility for policy coordination.

Section 4: Information-Sharing: (a) Requires the Director of National Intelligence ("DNI"), the Attorney General, and the Secretary of DHS to timely produce unclassified versions of all cyber threat

reports that identify a specific targeted entity; (b) directs the DNI, Attorney General, and Secretary of DHS to establish a procedure that includes the dissemination of classified reports to critical infrastructure entities authorized to receive them; (c) instructs DHS, in collaboration with DoD, to allow CI owners and operators in all sectors to participate in the Enhanced Cybersecurity Services initiative, an expanded version of the current DIB program, through which the government furnishes classified cyber threat information to participating companies; (d) in order to facilitate information-sharing, requires DHS to expedite the provision of security clearances to appropriate CI employees.

Section 5: Privacy and Civil Liberties Protections: (a) Requires the DHS Chief Privacy Officer and Officer for Civil Rights and Civil Liberties to make annual reports on ways to mitigate the privacy and civil rights risks of the initiatives authorized by the Order; (b) requires all participating agencies to coordinate their activities with their privacy and civil liberties officials.

Section 6: Consultative Process: Directs the Secretary of DHS to establish a consultative process using the Critical Infrastructure Partnership Advisory Council and Sector Coordinating Councils (private sector councils with representatives from owners and operators within sectors of CI identified by the National Infrastructure Protection Plan), CI owners and operators, agencies, independent regulatory agencies, state, local, territorial, and tribal governments, universities, and outside experts.

Section 7: Baseline Framework to Reduce Cyber Risk to Critical Infrastructure: Directs NIST to coordinate the development of a "technology-neutral" set of cybersecurity performance standards, known as the "Cybersecurity Framework," through a public comment process. The Framework is to include "standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks," and to incorporate consensus-based standards, industry best practices, and international standards to the extent possible. The Framework will focus on cross-sector standards, while identifying areas for improvement to be addressed at the sector-specific level. The Framework is to be updated "as necessary" based on technological changes, changes in cyber risks, feedback from owners and operators of CI, and experience with the Voluntary Critical Infrastructure Cybersecurity Program.

Section 8: Voluntary Critical Infrastructure Cybersecurity Program: (a) Directs DHS and Sector-Specific Agencies to establish a voluntary program for owners and operators of CI (and other interested entities) to adopt the Framework; (b) instructs the Sector-Specific Agencies to review the Framework with Sector Coordinating Councils, develop any necessary guidance to address sector-specific concerns, and annually report to the President the participation rate of owners and operators of CI at greatest risk; (c) instructs the Departments of Treasury and Commerce to recommend to the President incentives to encourage CI participation, both under existing law and those requiring legislation; (d) directs DoD and GSA, in consultation with the Federal Acquisition Regulatory Council, to advise the President on the merits of incorporating security standards into "acquisition planning and contract administration."

Section 9: Identification of Critical Infrastructure at Greatest Risk: Directs DHS to use a risk-

based approach to identify CI "where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." DHS is to use consistent, objective criteria in making these determinations, and shall not identify any "commercial information technology products or consumer information technology services." These identifications are to be reviewed and updated annually, in light of information from relevant agencies and stakeholders. DHS shall: (a) notify all identified CI owners and operators confidentially; (b) provide owners and operators of identified CI with relevant threat information; (c) establish a process whereby notified CI owners and operators may submit relevant information and request reconsideration of the identification.

Section 10: Adoption by Agencies: Directs regular departments and agencies with responsibilities for regulating CI security (and encourages independent regulatory agencies with such responsibilities) to review the cybersecurity framework and determine if current cybersecurity regulatory requirements are sufficient to meet current and projected risks. In making these determinations, regular agencies are to consider the identification of CI at greatest risk. Such agencies shall report to the President: (i) whether the agency has "clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risk to [CI]"; (ii) the existing authorities identified; (ii) any additional authority required; and (iv) the extent to which existing requirements overlap, conflict, or could be harmonized. If current authorities are insufficient, regular agencies shall propose "prioritized, risk-based, efficient, and coordinated actions," possibly including new rules establishing mandatory requirements, to mitigate cyber risks.

Legislative Outlook

An important immediate impetus for the Executive Order is the stalemate over cybersecurity legislation on Capitol Hill, a stalemate attributable in considerable part to controversy over establishment of additional cybersecurity standards for CI. Leaders in the previous Congress indicated that cybersecurity legislation would be a high priority, but omnibus legislation was blocked twice in the Senate and never reached the floor in the House. In the face of increased cyber risk and gridlock on the Hill, the President has used existing authorities to advance the goal of increased CI cybersecurity.

The issuance of the Executive Order may temper the sense of urgency on Capitol Hill to enact broad cybersecurity legislation but piecemeal legislative efforts, particularly aimed at enhancing information-sharing both within the private sector and between the private sector and the government, will likely continue. Just today, Rep. Mike Rogers (R-MI), Chair of the House Select Committee on Intelligence, and Ranking Member Rep. Dutch Ruppersberger (D-MD), will be introducing a bill similar to the Cyber Intelligence Sharing and Protection Act ("CISPA"), which passed the House 248-168 in the last Congress, despite a veto threat. CISPA would have given qualified companies access to classified cyber threat data from the intelligence community, immunized companies and their cybersecurity providers from liability for good faith using and

sharing of such information in aid of cybersecurity efforts, and created incentives for companies to share information with the government.

---

[1] The Executive Order is available at http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[2]A fuller description of the SEC guidance can be found here.

Authors

Jamie Gorelick

PARTNER

Chair, Regulatory and Government Affairs Department

jamie.gorelick@wilmerhale.com

+1 202 663 6500

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770