VENABLE® LLP

Cybersecurity Alert

February 2013

Executive Order Opens Consultative Processes to Draft Cybersecurity Framework for Critical Infrastructure

AUTHORS

Michael J. Baader
Jamie Barnett, Rear Admiral (Ret.)
Raymond V. Shepherd, III
Anthony J. Rosso
Robert L. Smith, II
Brian M. Zimmet
Dismas Locaria
Kathryn K. Floyd
Andrew E. Bigart
Jason R. Wool
Sejal C. Shah
Amanda C. Blunt

RELATED PRACTICES

Privacy and Data Security
Homeland Security
Legislative and Government Affairs
Corporate

ARCHIVES

2013 2009 2005
2012 2008 2004
2011 2007 2003
2010 2006

On February 12, 2013, President Obama signed an **Executive Order** aimed at enhancing the security of U.S. critical infrastructure by establishing a voluntary program for the adoption of cybersecurity standards to protect critical infrastructure, as well as a public-private partnership for information sharing.

The Executive Order focuses on three themes: (1) information sharing, (2) privacy, and (3) standards and best practices. Each of these could significantly affect companies in sectors associated with critical infrastructure, as well as any business that relies heavily on the Internet.

This alert seeks to answer questions that owners and operators of critical infrastructure may have regarding the Executive Order and how they may participate in the development of cybersecurity standards and policy moving forward.

What Is Critical Infrastructure?

Section 2 of the Executive Order relies on the definition of "critical infrastructure" from the USA PATRIOT Act of 2001: systems or assets, whether physical or virtual, so vital to the U.S. that their incapacity or destruction would have a debilitating impact on national security, economic security, public health or safety, or any combination thereof.

Examples of critical infrastructure include:

- Owners of electricity generation, transmission, and distribution facilities;
- Oil and gas production, transport, and distribution facilities;
- Cable, wireless, and other telecommunication operators;
- Public health facilities (hospitals, EMS, etc.);
- Water supply facilities; and
- Financial services (banks, ATMs, etc.).

Within 150 days of the Executive Order date, the Secretary of Homeland Security must consult with private industry and use objective criteria to identify "high-risk critical infrastructure," defined as entities for which "a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

Following the consultative process, the Secretary must confidentially notify owners and operators of identified high-risk critical infrastructure and ensure they are provided with relevant cyber threat information.

How Will the Federal Government and Private Sector Share Cyber Threat Information?

To "increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities," the Executive Order requires the rapid dissemination to targeted entities of unclassified versions of all reports of cyber threats to the U.S. that identify a specific entity. Pursuant to the same process, authorized critical infrastructure entities may also receive classified reports. Further:

- To support this information sharing, the Secretary will expedite the provision of security clearances to appropriate personnel of critical infrastructure owners and operators, with priority for high risk entities, as defined in Section 9 of the Order.
- Within 120 days of the Executive Order's date of issuance, the Secretary of Homeland Security, in coordination with the Secretary of Defense, must establish procedures to expand the Enhanced Cybersecurity Services initiative (ECS) to all critical infrastructure sectors. ECS is a voluntary program through which the Department of Homeland Security and Commercial Service Providers share indicators of malicious cyber activity. ECS indicator reports vary in detail and relate to IP addresses, domains, E-mail headers, files, and strings that pose a threat to network security. A Memorandum of Agreement (MOA) currently governs the government's handling and use of

information shared through ECS.

How Will the Government Protect Cyber Threat Information Shared by the Private Sector?

The Executive Order provides that threat information regarding critical infrastructure security submitted by private entities to a federal agency shall be protected from disclosure to the fullest extent permitted by law. This provision exempts cyber threat information voluntarily shared with the federal government from Freedom of Information Act (FOIA) requests, agency *ex parte* communication prohibitions, and other disclosure requirements.

Will the Federal Government Establish Cybersecurity Standards as Part of a National Framework?

Yes. While these standards have not yet been developed, the Executive Order requires the National Institute of Standards and Technology (NIST) to lead the development of a Cybersecurity Framework. The Cybersecurity Framework will include standards, methodologies, procedures, and processes to help owners and operators of critical infrastructure identify, assess, and manage cyber risk with a cost-effective, flexible approach. Adoption of the Cybersecurity Framework is currently voluntary, however, Section 10(a) of the Order requires that within 90 days of publication of the preliminary Framework, agencies must submit a report to the President stating whether the agency has clear authority to establish requirements based upon the Framework, any additional authority required, and the extent to which the agency's existing requirements overlap, conflict, or could be harmonized. Thus, it appears that the issuance of binding regulations related to the Framework is a real possibility.

Will the Private Sector Have an Opportunity to Participate in Developing Cybersecurity Standards?

Yes. Section 7 directs NIST to engage in an open public review and comment process as part of the development of the Framework, as well as the consultation of owners/operators of critical infrastructure and other stakeholders through a consultative process established in Section 6. To this end, NIST issued a **Request for Information** (RFI), which will also be published in the *Federal Register*, to collect information from the public regarding the "many interrelated considerations, challenges, and efforts needed to develop" the Cybersecurity Framework.

In addition, NIST will host a series of informational meetings and workshops "to gather additional input and develop the Framework." Using these workshops and the RFI, NIST states that it will (i) identify existing cybersecurity standards, guidelines, frameworks, and best practices that are applicable to increase the security of critical infrastructure sectors and other interested entities; (ii) specify high-priority gaps for which new or revised standards are needed; and (iii) collaboratively develop action plans by which these gaps can be addressed.

The electric utility industry and federal contractors may be uniquely positioned to influence this process and/or assist owners and operators in meeting any such standards given the fact that the industry is already subject to cybersecurity regulation and oversight. For more information, see ***Cybersecurity regulation: 5 issues for companies***.

The Director of NIST will publish the preliminary Framework within 240 days of the Executive Order date and the final Framework within one year. The Director will review and update the Framework as necessary.

Will There Be Incentives to Adopt the Framework?

Yes. The Secretary will establish a voluntary program to support the implementation of the Framework, in coordination with Sector-Specific Agencies and Sector Coordinating Councils, as defined by Presidential Policy Directive 21, "**Critical Infrastructure Security and Resilience**," also signed on February 12 in conjunction with the Order. The Order directs the Secretary to coordinate the establishment of incentives to promote participation in this program. Within 120 days of the Order, the Secretaries of Homeland Security, Commerce, and Treasury will each make recommendations to the President analyzing the benefits and relative effectiveness of these incentives, as well as whether they could be provided under existing legal authority. These incentives may include tax breaks, subsidies, or preference programs such as the Customs-Trade Partnership Against Terrorism (C-TPAT).

Will the Framework Affect Federal Procurement?

Most likely. Within 120 days of the Order, the Secretary of Defense and the Administrator of General Services, in consultation with the Federal Acquisition Regulatory Council, will make recommendations to the President on the feasibility, security benefits, and relative merits of incorporating security

standards into acquisition planning and contract administration.

This will not necessarily be new to federal procurement, as the Department of Defense and General Services Administration, to name a few, **have already implemented cybersecurity standards** for certain types of procurements. In addition, the 2013 National Defense Authorization Act requires certain cybersecurity actions by defense contractors.

What's Next for Interested Parties?

While the President's Executive Order leaves much to be decided and worked out through the regulatory process, it is clear that cyber regulation has arrived and will likely continue to grow and evolve over time.

In this respect, the Executive Order is only the starting point in the development of a comprehensive national cybersecurity framework. Moving forward, federal agencies will seek to implement the President's directive by issuing new rules and policies, most of which will be subject to public review and comment. Not to be left out, several members of Congress have announced plans to reintroduce either comprehensive or "wrap-around" cybersecurity legislation that stalled last year. These two tracks will move forward together, with each offering interested parties multiple opportunities to impact final policy.

Owners and operators of critical infrastructure should be mindful of this new wave of voluntary regulation, and consider involving themselves in the dialogue and discourse that will ensue. Indeed, industry participation at this stage, while the landscape is voluntary and under development, offers many more opportunities to frame the debate. Venable expects to track and actively participate in the NIST workshops and draft RFI responses on behalf of its clients.

For more information on the Executive Order, the NIST workshops and RFI responses, or cybersecurity regulation generally, please feel free to contact any of the above listed authors.

Venable LLP offers a broad array of legal services to a variety of different players within the cybersecurity arena. Our attorneys are adept at understanding complex client issues and tapping into the extensive experience of our many practice areas including privacy and data security, e-commerce, intellectual property and government contracting.