

Obama Administration Moves Forward on Cybersecurity

Andrew Art, Jonathan Simon, and Michael O'Neill

On February 12, 2013, citing congressional inaction, President Obama issued a much anticipated executive order to help address cyber threats and attacks on the nation's infrastructure. The Executive Order [Improving Critical Infrastructure Cybersecurity](#) (Executive Order) establishes federal government initiatives to improve the sharing of information related to cyber threats between the federal government and owners and operators of critical infrastructure, and to develop and implement a framework based on voluntary, risk-based standards to reduce cyber risks to critical infrastructure.


An accompanying [Presidential Policy Directive](#) (Directive) establishes national policy and describes three strategic imperatives for federal agencies, including: (1) refining and clarifying functional relationships across the federal government to strengthen critical infrastructure security and resilience; (2) enabling effective information exchange by identifying baseline data and systems requirements for the federal government; and (3) implementing an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

The Executive Order will likely affect and may involve participation by owners and operators of electric utilities, natural gas pipelines, dams, nuclear facilities, financial services, critical manufacturing, transportation systems, water and wastewater facilities, and health care facilities, among other critical infrastructure.

NEW CYBERSECURITY ACTIONS

Information Sharing

The Executive Order specifies several changes intended to improve the sharing of information concerning cyber threats and vulnerabilities among the federal government, state and local governments, and private industry. The Executive Order directs the Department of Homeland Security (DHS) to expand the Enhanced Cybersecurity Services program from the Defense Industrial Base to all critical infrastructure sectors by June 12, 2013. This program is DHS's voluntary information sharing program that provides classified cyber threat and technical information to "eligible critical infrastructure companies or commercial service providers." The Executive Order further instructs the Attorney General, DHS, and the Director of National Intelligence to establish processes to produce unclassified reports of cyber threats that identify a specific targeted entity and to rapidly disseminate those reports to any targeted entity. In addition, the Executive Order requires DHS to expedite the processing of security clearances for personnel employed by critical infrastructure owners or operators, as well as to expand the use of programs that bring private sector subject matter experts into federal service on a temporary basis to obtain advice on the information most useful to critical infrastructure owners and operators for reducing and mitigating cyber risks.



Cybersecurity Framework

The Executive Order requires the Department of Commerce, through its National Institute of Standards and Technology (NIST), to develop a Cybersecurity Framework to reduce cyber risks to critical infrastructure. The Cybersecurity Framework will include cybersecurity standards, methodologies, procedures, and processes applicable to critical infrastructure across all sectors, as well as performance metrics for entities adopting and implementing the framework. The Cybersecurity Framework will be developed through an open public review and comment process, and in consultation with federal agencies, owners and operators of critical infrastructure, and other stakeholders. Adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other entities is to be voluntary, although the Executive Order directs DHS to coordinate establishment of incentives to promote participation in the program.


Federal agencies with regulatory responsibility, other than the Federal Energy Regulatory Commission (FERC) and other independent regulatory agencies, are required to collaborate to ensure that their regulations are sufficient to mitigate the risks of cybersecurity failures. Participation from these agencies will come in two steps. Once a preliminary draft of the Cybersecurity Framework is released, by October 11, 2013, federal agencies charged with protecting critical infrastructure are required to produce a report on whether or not the agency has sufficient legislative or executive authority to establish any additional regulations based upon the Cybersecurity Framework. The Executive Order encourages, but does not require, DHS to consult with independent agencies such as FERC, which has jurisdiction over mandatory reliability standards that apply to the electric sector in the lower 48 states.

Once the final Cybersecurity Framework is published, the relevant federal agencies must propose any additional cybersecurity regulations to bring their regulatory regime into alignment. Under the Executive Order, the final Cybersecurity Framework is to be completed by February 12, 2014, and agencies must propose any additional regulatory action within 90 days, by May 19, 2014. The Executive Order requires that these additional regulations be “prioritized, risk-based, efficient, and coordinated actions.”

Identifying Critical Infrastructure at “Greatest Risk”

The Executive Order requires that, by July 12, 2013, the Secretary of Homeland Security, with input from sector-specific agencies and private industry, use risk-based criteria to identify “critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.” After the Secretary determines the specific critical infrastructure at greatest risk, DHS will confidentially notify owners and operators of the listed facilities that their facilities have been identified. Owners and operators of identified facilities will have an opportunity to request reconsideration of the Secretary’s determination. The Executive Order precludes the Secretary from identifying “commercial information technology products or consumer information technology services” as critical infrastructure.

The Executive Order and the Directive also require that sector-specific agencies provide assistance and information to help DHS determine which systems belong on the critical infrastructure list. The agencies will also be responsible for submitting an annual report to the President detailing the extent to which owners and operators of identified critical infrastructure systems are participating in the voluntary program to support the Cybersecurity Framework.



The Directive lists nine agencies that will be responsible for 16 designated critical infrastructure sectors.

Reports and Processes

Finally, the Executive Order and the Directive set forth a process to coordinate the development of cybersecurity standards and programs by mandating the production of various reports and deliverables over the coming year. The Directive requires that six reviews be completed over the coming two years and the Executive Order provides a range of steps for cybersecurity policy development and review with the input of both government and non-governmental stakeholders.

INITIAL AGENCY IMPLEMENTATION

Following the issuance of the Executive Order, NIST immediately initiated a process for developing the Cybersecurity Framework. On February 13, NIST [announced](#) that it will issue a Request for Information (RFI) to solicit information on existing standards and industry “best practices” from the owners and operators of critical infrastructure systems, federal agencies, state and local governments, and other stakeholders.

NIST intends to base its standards development process on the process used to set standards for Smart Grid and secure cloud computing technologies. Across sectors, NIST will seek information on topics including: encryption and key management; asset identification and management; and security engineering practices. The Cybersecurity Framework also will include performance metrics that assess whether the risks of disruption from cybersecurity incidents are effectively mitigated by the practices adopted and the Cybersecurity Framework as a whole.


The preliminary summary of the RFI indicates that NIST will focus its information collection efforts on three main areas:

- 1) Current risk management practices, including cyber threat risk assessment;
- 2) The applicability of current standards published by international standards organizations, the U.S. Government, state agencies, industry, or other interested parties; and
- 3) Industry-specific practices, such as separation of business and operational systems, use of encryption, incident handling procedures, system resiliency practices, and privacy protection.

The NIST process is moving very rapidly, with only 45 days allotted for industry responses to be submitted to the RFI after its publication in the Federal Register.

IMPLICATIONS

The Executive Order takes important steps to enhance coordination and the sharing of federal cybersecurity threat information between government and private industry. The Executive Order, however, was not intended to replace congressional action and does not preclude the need for such action. Statutory changes remain necessary, for



instance, to address Freedom of Information Act and other privacy concerns that continue to limit the sharing of private industry’s proprietary information with federal agencies, and to otherwise facilitate information sharing and access to classified information.

The NIST Cybersecurity Framework has the potential to create new performance metrics and regulatory requirements with legal consequences for owners and operators of critical infrastructure. In addition, specifically for the electric sector, the NIST standards-based framework also has the potential to result in standards that overlap and potentially conflict with the current mandatory North American Electric Reliability Corporation (NERC) reliability standards. For example, NIST intends to include within the Framework “metrics, methods, and procedures that can be used to assess and monitor... the effectiveness of security controls” and establish a “comprehensive risk management approach that provides the ability to assess, respond to, and monitor information security-related risks.” The NERC critical infrastructure protection standards that now apply to owners and operators of designated critical cyber assets also address similar security controls and measures and have already required the development of company-specific plans and procedures for many utilities in the electric sector. To avoid the creation of a patchwork of potentially overlapping and conflicting reliability standards, it is particularly important for utilities in the electric sector to participate actively in the processes NIST develops to create the Framework.

The Executive Order will result in the identification and confidential listing of the critical infrastructure with the greatest risk to the health and prosperity of the United States. Even if the listing of the identified facilities remains confidential within government and is never leaked, the owners and operators of listed critical infrastructure are likely to face new federal oversight and scrutiny of their cybersecurity programs.

FOR ADDITIONAL INFORMATION

Van Ness Feldman counsels electric utilities, natural gas pipelines, and other owners and operators of critical infrastructure on reliability and safety standards and other matters. For assistance or additional information, please contact [Andrew Art](#) or [Jonathan Simon](#) at (202) 298-1800 in Washington, D.C. We also invite you to follow Van Ness Feldman’s Electric Practice at <http://twitter.com/VNFelectric>.

In February 2012, Van Ness Feldman expanded its capabilities by combining practices with the Seattle law firm of GordonDerr LLP, a preeminent real estate, land use, water law, and civil litigation firm in the Pacific Northwest. Learn more at www.vnf.com.

© 2013 Van Ness Feldman, LLP. All Rights Reserved.

This document has been prepared by Van Ness Feldman for informational purposes only and is not a legal opinion, does not provide legal advice for any purpose, and neither creates nor constitutes evidence of an attorney-client relationship.