Morgan Lewis

alert

energy lawflash

February 14, 2013

President Obama Signs Executive Order on Cybersecurity

Order will create a voluntary Cybersecurity Framework for designated critical infrastructure within a year.

On February 12, President Barack Obama signed an executive order[1] directing the Department of Homeland Security (DHS) to identify critical infrastructure and encourage the designated owners and operators of critical infrastructure to adopt a voluntary cybersecurity program that will be developed by the National Institute of Standards and Technology (NIST). As reflected in the president's State of the Union address,[2] DHS is certain to identify electric system infrastructure as critical, resulting in significant pressure on electric utilities to adopt the NIST standards.

DHS to Identify Critical Infrastructure

Over the next five months, DHS is tasked with using a risk-based approach to identify critical infrastructure that, if subject to a cyber attack, could have "catastrophic" effects on health, safety, the economy, or national security. For the energy sector, DHS must consult with the Department of Energy (DOE), as well as relevant stakeholders, including the owners and operators of critical infrastructure. The nuclear industry is carved out of DOE oversight, but DHS serves as the designated "sector-specific agency" for nuclear critical infrastructure.

Once DHS identifies what it considers to be critical infrastructure, it will privately notify the relevant owners and operators of its determination and provide an explanation for its decision as well as an opportunity for the asset owners and operators to seek reconsideration.

NIST to Develop Voluntary Standards

The owners and operators of the identified critical infrastructure will then be encouraged to adopt a voluntary framework of cybersecurity protections (termed the "Cybersecurity Framework") that NIST will develop over the course of the next year through a notice-and-comment process. The Cybersecurity Framework is intended to draw upon voluntary consensus standards and current industry best practices, to the extent possible, in developing "standards, methodologies, procedures, and processes" for addressing cyber risks. The Cybersecurity Framework is intended to assist, in a technologically neutral manner, owners and operators of critical infrastructure in determining, analyzing, and managing the cyber risks to their protected assets. It will also include measures for assessing ongoing compliance with the Cybersecurity Framework.

Although NIST is required to develop the Cybersecurity Framework through a consultative process with stakeholders, including the various federal, state, and local agencies and the asset owners and operators, the executive order also provides for explicit public comment procedures. Within eight months, NIST must publish a preliminary Cybersecurity Framework, and the final Cybersecurity Framework will be due within a year.

1. View the executive order at http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

2. In his February 12 State of the Union address, President Obama stated that the growing threat from cyber attacks was his reason for issuing the executive order "that will strengthen our cyber defenses by increasing information sharing, and developing standards to protect our national security, our jobs, and our privacy." View the full State of the Union address at http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address.

DHS Program to Encourage Adoption of Voluntary Standards

Once NIST finishes developing the Cybersecurity Framework, DHS must develop a voluntary Cybersecurity Framework compliance program for the owners and operators of designated critical infrastructure. The executive order anticipates that the sector-specific agencies, such as DOE, will then develop sector-specific guidance that adapts the NIST Cybersecurity Framework to the relevant industry.

Recognizing that DHS cannot impose traditional legal compliance obligations in the absence of new legislation, the executive order directs the sector-specific agencies to report to the president each year on whether the owners and operators of critical infrastructure in their sectors are implementing the Cybersecurity Framework. DHS will also look for other ways to incentivize compliance under existing law. Finally, the executive order directs the relevant agencies to determine whether the Cybersecurity Framework could be incorporated into federal contracting obligations.

To determine the possibility of enacting the voluntary standards as mandatory requirements, the executive order directs the agencies with authority over critical infrastructure to report to the president, within three months of the preliminary Cybersecurity Framework's publication, on whether they have the authority to require the implementation of the Cybersecurity Framework.

Information Sharing on Cyber Threats to Be Improved

The executive order also addresses the need for increased information sharing with private industry about threats to critical infrastructure identified by the intelligence community. Under the order, intelligence agencies will be required to improve their ability to share threat information with targeted entities in both unclassified reports and classified threat information. This information will be shared with individuals at targeted entities who have the appropriate authorizations. The executive order directs DHS to expedite its processing of security clearances to make that sharing possible.

Contacts

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following Morgan Lewis attorneys:

Washington, D.C.

Stephen M. Spina	202.739.5958	sspina@morganlewis.com
J. Daniel Skees	202.739.5834	dskees@morganlewis.com

About Morgan, Lewis & Bockius LLP

With 24 offices across the United States, Europe, and Asia, Morgan Lewis provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. Our international team of lawyers, patent agents, benefits advisers, regulatory scientists, and other specialists—more than 1,600 legal professionals total—serves clients from locations in Almaty, Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Moscow, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.