Shook, Hardy & Bacon L.L.P.

FEBRUARY 13, 2013

DATA SECURITY ALERT

THE WHITE HOUSE EXECUTIVE ORDER ON CYBERSECURITY

Yesterday, President Obama issued an Executive Order that attempts to improve critical infrastructure cybersecurity in the United States by requiring certain federal agencies to share classified cyber threat information with critical infrastructure companies in an effort to develop voluntary standards and procedures to limit the risk associated with these threats.

The Order, which became effective during the President's State of the Union address on February 12th, requires the following:

- Within 120 days, the Attorney General, the Secretary of Homeland Security (Secretary), and the Director of National Intelligence must each issue instructions to ensure the timely production and rapid dissemination of unclassified reports of cyber threats to the U.S. that identify a specific targeted entity.
- Within 120 days, the Secretary shall establish procedures to implement an Enhanced Cybersecurity Services Program for all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure. The Order envisions a "consultative process" between federal agencies and the private sector to coordinate improvements to the cybersecurity of critical infrastructure.
- The federal government must identify companies it considers to be critical infrastructure owners and operators within 150 days. In making this determination, the government will look to whether a cybersecurity incident affecting that company could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.
- Security clearance will be expedited for employees of critical infrastructure owners and operators.

Shook, Hardy & Bacon understands companies face challenges securing information in an increasingly electronic world.

SHB guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage risks associated with maintaining and using electronic information.

For more information on SHB's data security and data privacy services, please contact:

Al Saikali
(305) 960-6923
asaikali@shb.com

Thérèse Miller
(415) 544-1965
tpmiller@shb.com

- Programs that bring private sector subject-matter experts into federal service on a temporary basis will be expanded, so that those individuals can provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.
- Federal agencies are required to coordinate activities under the Order to ensure that privacy and civil liberties protections are incorporated into their activities.
- Information submitted voluntarily by private entities under the Order must be protected from disclosure.

So how will this new program be implemented? The National Institute of Standards and Technology will publish a framework to reduce cyber risks to critical infrastructure. The framework must do the following:

- Include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.
- Incorporate voluntary consensus standards and industry best practices to the fullest extent possible.
- Be consistent with voluntary international standards when such international standards will advance the objectives of the Order, and shall meet the requirements of certain federal legislation.
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.
- Focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure.
- Identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations.
- Provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks.
- Include guidance for measuring the performance of an entity in implementing the framework.

- Include methodologies to identify and mitigate impacts of the framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.
- The Secretary must establish a Voluntary Critical Infrastructure Cybersecurity Program to support the adoption of this framework.

At this point in time, the Order creates more questions than answers, due in part to the broad language it must use. For example, what will these voluntary standards be and for how long? Even if the standards are "voluntary", what company would refuse to comply with them given the affect noncompliance could have on their reputation? Who will be identified as critical infrastructure operators? Will these standards become the new standard for determining whether a non-critical infrastructure company's security measures are "reasonable"? Finally, will the Order be challenged as unconstitutional on separation of powers grounds (i.e., to what extent is the Order an invasion of Congress's power to make law)?

The Executive Order can be found here.

For more information about these and other issues relating to data security law, visit Al's blog at www.datasecuritylawjournal.com.

OFFICE LOCATIONS

Geneva, Switzerland
+41-22-787-2000
Houston, Texas
+1-713-227-8008
Irvine, California
+1-949-475-1500
Kansas City, Missouri
+1-816-474-6550
London, England
+44-207-332-4500
Miami, Florida
+1-305-358-5171
Philadelphia, Pennsylvania
+1-215-278-2555
San Francisco, California
+1-415-544-1900
Tampa, Florida
+1-813-202-7100
Washington, D.C.
+1-202-783-8400