LOEB & LOEB LLP

Privacy Law
ALERT
MARCH 2013

LOEB & LOEB adds Knowledge.

President Issues Cybersecurity Executive Order; Pending Legislation Revived

President Barack Obama issued his administration's much-anticipated executive order on cybersecurity Feb. 12, 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." While the order does not have the power of a legislative action and does not require the private sector to take any action, it does create a voluntary partnership between the owners and operators of critical infrastructure and the government to improve information sharing, to develop and implement risk-based standards, and to evaluate the current regulatory landscape in light of increased cybersecurity threats. In addition, the order requires government agencies and executive officials, including the Secretary of Defense and Secretary of Homeland Security (Secretary), to take specific actions, such as sharing information with private sector entities to enable them to protect against threats to the critical infrastructure; creating a framework of standards and best practices to protect the critical infrastructure; and proposing any actions necessary to properly implement the framework.

Private Sector Impact

A threshold issue for companies in the private sector is whether their organizations are part of the critical infrastructure. The order defines "critical infrastructure" very broadly 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." Beyond the more obvious industry sectors – defense-related, financial, energy, transportation, health care and security – the definition potentially could include Internet-based systems across a broad spectrum of industries and economic sectors. The Department of Homeland Security's list of critical infrastructure sectors lists 18 different sectors, including, among others, food and agriculture, banking and finance, commercial facilities, communications, information technology, critical manufacturing, defense industrial base, energy and nuclear power, postal and shipping, health care, and transportation. The order may impact not only organizations in those sectors, which are also broadly delineated, but also organizations that provide services to those sectors.

In addition, Section 9 of the order requires the Secretary of Homeland Security to determine, in consultation with other agencies and the private sector, critical infrastructure for which a cybersecurity incident would have catastrophic regional or national effects on public health or safety, economic security, or national security. The order expressly states that commercial or consumer information technology products are not included in this priority critical infrastructure. The Secretary will confidentially notify owners and operators of critical infrastructure that they have been identified through the process outlined in Section 9 and will provide them with the basis for the determination, as well as a process through which to submit relevant information and request reconsideration of designation. The Secretary will review, update and send the list to the President annually.

Information Sharing

To enable private sector entities to protect against threats to critical infrastructure, the executive order requires key government agencies to increase the amount, quality and timeliness of information about cyberthreats shared with the private sector. The U.S. attorney general, the Secretary, and the Director of National Intelligence must establish processes to produce reports on unclassified cyber threats that identify

a specific targeted entity and to disseminate these reports rapidly to targeted entities. In addition, the Enhanced Cybersecurity Services Program, a voluntary information-sharing program that historically enabled the sharing of classified cyber threat information from the government to companies mainly in the defense sector, will be expanded to include all critical infrastructure sectors.

Voluntary Standards to Reduce Cyberrisks

In an effort to alleviate private sector concerns over increased regulation while still addressing the need for improved cybersecurity, the executive order directs the creation of a "Cybersecurity Framework" and the "Voluntary Critical Infrastructure Cybersecurity Program" for the implementation of that framework in the private sector.

The Cybersecurity Framework will include standards, processes and procedures developed by the National Institute of Standards and Technology and incorporating, to the extent possible, voluntary consensus standards and industry best practices. The order describes the framework as 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" and includes cross-sector security standards and guidelines. The order requires NIST to publish a preliminary Cybersecurity Framework within 240 days of the order and a final version of the Cybersecurity Framework within one year of the order.

The order calls on the Secretary, with assistance from sector-specific and other relevant agencies, to develop the Voluntary Critical Infrastructure Cybersecurity Program to support the adoption of the Cybersecurity Framework by the owners and operators of the critical infrastructure. The Secretary is also tasked with coordinating the establishment of incentives designed to promote participation in the Program. The order particularly focuses on the participation of owners and operators of high-risk infrastructure identified under Section 9 in the Program.

Legislative and Regulatory Landscape

The order specifically contemplates the development of legislation and regulations that could result in making the voluntary cybersecurity standards mandatory. The Department of Homeland Security, the Office of Management and Budget, and the national security staff must review the preliminary Cybersecurity Framework to determine whether current cybersecurity regulatory requirements are sufficient to address current and projected cyberrisks, focusing particularly on the priority infrastructure designated under Section 9, and must report to the president on whether these agencies have the authority to establish mandatory requirements based on the Cybersecurity Framework. To the extent that inadequacies are identified, the agencies must also propose "prioritized, risk-based, efficient, and coordinated actions" to mitigate cyberrisk. The order also specifically contemplates private sector involvement in the evaluation of existing and proposed cybersecurity regulation.

Privacy and Civil Liberty Considerations

The executive order directly addresses privacy considerations in Section 5, specifically requiring the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security, in consultation with the Privacy and Civil Liberties Oversight Board and the Office of Management and Budget, to assess the privacy and civil liberties risks of the agency's actions and programs under the order and to recommend – in a publicly available report – ways to minimize or mitigate those risks. Other agencies acting under the order must provide similar assessments to the Department of Homeland Security. Those assessments will also be included in the report, to be released in February 2014 and reviewed and amended on an annual basis. Agencies acting under the order are also required to consider the assessments and recommendations in implementing privacy and civil liberties protection.

The order also expressly provides that any information voluntarily submitted by companies in accordance with federal law 6 U.S.C. Sec. 133, Protection of voluntarily shared critical infrastructure information, will be protected from disclosure "to the fullest extent permitted by law" Section 133 provides, among other protections, that this information is not subject to disclosure in reply to a Freedom of Information Act request or any state or local law governing information disclosures; that it may not be used, without consent, by governmental agencies or third parties in civil litigation; and that it does not constitute a waiver of any privilege or protection, such as trade secret protection.

Section 7, governing the development of the Cybersecurity Framework, also specifically provides that the Framework include methods to protect individual privacy and civil liberties as well as to identify and mitigate the impact on business confidentiality.

Takeaways

Recent headlines about cybersecurity breaches and President Obama's Executive Order have renewed the focus on the issue of cyberthreats and the protection of critical infrastructure. Immediately following the announcement of the Executive Order, proponents of the controversial

Cyber Intelligence Sharing and Protection Act, known as CISPA, reintroduced the bill (H.R. 624) in the House of Representatives, saying that the president's order, while a good start, did not go far enough in protecting businesses from cyberthreats. The bill passed the House in 2012 but died in the Senate after the President, citing privacy concerns among other issues, indicated he would veto the bill. CISPA would permit federal government agencies to share cyberthreat information with any private sector entity and would also let businesses share cyberthreat information with other companies and the government.

Under the voluntary framework contemplated by the executive order, and in the absence of any federal or state regulations, companies covered by the order are vulnerable. Even though the executive order specifically states that the order is not intended to "create any right or benefit, substantive or procedural, enforceable at law or in equity by any party," companies that voluntarily report under the order may not be protected from any potential liability stemming from their reporting. In addition, even though compliance with the order's Cybersecurity Framework is voluntary, failure to comply may leave companies open to private actions if they suffer a cybersecurity or data breach.

Advanced Media and Technology Department

KENNETH A. ADLER	KADLER@LOEB.COM	212.407.4284
ROBERT M. ANDALMAN	RANDALMAN@LOEB.COM	312.464.3168
ALISA C. BERGSTEIN	ABERGSTEIN@LOEB.COM	312.464.3155
IVY KAGAN BIERMAN	IBIERMAN@LOEB.COM	310.282.2327
CHRISTIAN D. CARBONE	CCARBONE@LOEB.COM	212.407.4852
TAMARA CARMICHAEL	TCARMICHAEL@LOEB.COM	212.407.4225
MARC CHAMLIN	MCHAMLIN@LOEB.COM	212.407.4855
MARGARET CHARENDOFF	MCHARENDOFF@LOEB.COM	212.407.4069
CRAIG A. EMANUEL	CEMANUEL@LOEB.COM	310.282.2262
KENNETH R. FLORIN	KFLORIN@LOEB.COM	212.407.4966
DANIEL D. FROHLING	DFROHLING@LOEB.COM	312.464.3122
NOREEN P. GOSSELIN	NGOSSELIN@LOEB.COM	312.464.3179
DAVID W. GRACE	DGRACE@LOEB.COM	310.282.2108
THOMAS A. GUIDA	TGUIDA@LOEB.COM	212.407.4011
NATHAN J. HOLE	NHOLE@LOEB.COM	312.464.3110
MELANIE J. HOWARD	MHOWARD@LOEB.COM	310.282.2143
MICHAEL W. JAHNKE	MJAHNKE@LOEB.COM	212.407.4285
THOMAS P. JIRGAL	TJIRGAL@LOEB.COM	312.464.3150
IEUAN JOLLY	IJOLLY@LOEB.COM	212.407.4810
JULIE E. LAND	JLAND@LOEB.COM	312.464.3161
JESSICA B. LEE	JBLEE@LOEB.COM	212.407.4073
MICHAEL MALLOW	MMALLOW@LOEB.COM	310.282.2287
KATHERINE THERESE MASON	KMASON@LOEB.COM	212.407.4898
DOUGLAS N. MASTERS	DMASTERS@LOEB.COM	312.464.3144
NERISSA COYLE MCGINN	NMCGINN@LOEB.COM	312.464.3130
ANNE KENNEDY MCGUIRE	AMCGUIRE@LOEB.COM	212.407.4143
DANIEL G. MURPHY	DMURPHY@LOEB.COM	310.282.2215
BRIAN NIXON	BNIXON@LOEB.COM	202.618.5013
ANGELA PROVENCIO	APROVENCIO@LOEB.COM	312.464.3123
CHRISTINE M. REILLY	CREILLY@LOEB.COM	310.282.2361
KELI M. ROGERS-LOPEZ	KROGERS-LOPEZ@LOEB.COM	310.282.2306
SETH A. ROSE	SROSE@LOEB.COM	312.464.3177
ROBERT MICHAEL SANCHEZ	RSANCHEZ@LOEB.COM	212.407.4173
ALISON POLLOCK SCHWARTZ	ASCHWARTZ@LOEB.COM	312.464.3169
STEVE A. SEMERDJIAN	SSEMERDJIAN@LOEB.COM	212.407.4218
BARRY I. SLOTNICK	BSLOTNICK@LOEB.COM	212.407.4162
REGAN A. SMITH	RASMITH@LOEB.COM	312.464.3137
BRIAN R. SOCOLOW	BSOCOLOW@LOEB.COM	212.407.4872
WALTER STEIMEL, JR.	WSTEIMEL@LOEB.COM	202.618.5015
AKIBA STERN	ASTERN@LOEB.COM	212.407.4235
JAMES D. TAYLOR	JTAYLOR@LOEB.COM	212.407.4895
MICHAEL A. THURMAN	MTHURMAN@LOEB.COM	310.282.2122
JILL WESTMORELAND	JWESTMORELAND@LOEB.COM	212.407.4019
DEBRA A. WHITE	DWHITE@LOEB.COM	212.407.4216
MICHAEL P. ZWEIG	MZWEIG@LOEB.COM	212.407.4960