MORRISON | FOERSTER

Morrison & Foerster Client Alert.

February 19, 2013

Cybersecurity Developments in the U.S. and the EU

By Nathan D. Taylor and Miriam H. Wugmeister

Everyone is talking about cybersecurity. Articles appear almost daily regarding significant cybersecurity events. And over the past two years, the drumbeat for action on the issue of cybersecurity and the protection of the nation's critical infrastructure has grown louder and louder. In the context of the current debate on cybersecurity, virtually everyone agrees that cyber threats are real, as evidenced by highly publicized cyber events, such as the recent denial of service attacks on banks. Virtually everyone also agrees that protecting critical infrastructure is an important goal. Nonetheless, little consensus has been reached, particularly in the U.S. Congress, on the "appropriate" approach to protecting the nation's critical infrastructure from cyber threats.

The U.S. Executive Branch and the EU Commission, however, have both now weighed in on the issue. President Obama's long-awaited and highly anticipated cybersecurity Executive Order ("Executive Order") was released on February 12, 2013, directing the U.S. government to take various steps to protect the nation's critical infrastructure from cyber threats.[1] Similarly, on February 7, 2013, the European Commission published a proposed Directive on network and information security for "market operators" (the "EU Directive").[2] The EU Directive, once finalized and transposed into Member State legislation, would apply to all "market operators" providing a service in the EU/EEA, including operators of critical infrastructure in the energy, transport, banking, finance, and health sectors, as well as "information society" service providers, such as e-commerce platforms, payment gateways, social networks, search engines, and cloud providers.

[1] The Order is available here. The President also released a related presidential policy directive establishing the nation's policy for the protection of critical infrastructure from all types of threats, which is available here.

[2] The draft Proposal for a Directive of the European Parliament and of the Counsel to ensure a high common level of network and information security across the Union COM(2013) 48 of February 7, 2013 is available here.

Beijing
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364

Hong Kong
Eric Dickinson 852 2585 0812
Gordon A. Milner 852 2585 0808

London
Ann Bevitt 44 20 7920 4041
Deirdre Moynihan 44 20 7920 4164
Anthony Nagle 44 20 7920 4029

Los Angeles
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Russell G. Weiss (213) 892-5640

New York
Madhavi T. Batliboi (212) 336-5181
John F. Delaney (212) 468-8040
Matthew R. Galeotti (212) 336-4044
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Northern Virginia
Daniel P. Westman (703) 760-7795

Palo Alto
Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

San Francisco
Roland E. Brandel (415) 268-7093
Anna Ferrari (415) 268-6728
Jim McCabe (415) 268-7011
James R. McGuire (415) 268-7013
William L. Stern (415) 268-7637

Tokyo
Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

Washington, D.C.
Nicholas A. Datlowe (202) 887-1590
Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Robert A. Salerno (202) 887-6930
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

While neither the Order nor the EU Directive are immediately or directly applicable to companies, they are indicative of the fact that legislation is likely coming around the world, and companies should begin to prepare now to comply with the key components of possible cybersecurity legislation.

THE EXECUTIVE ORDER

The Executive Order's clear purpose is to "enhance the security and resilience of the Nation's critical infrastructure." It attempts to do so by directing various federal agencies, including principally the Department of Homeland Security (DHS), to take a number of important steps designed to further this goal. In so doing, the Executive Order includes several important principles that were widely supported by the private sector, including provisions designed to improve the sharing of cyber threat information between the U.S. government and the private sector and improvements to the private-sector security clearance process. The Executive Order, however, also creates a regulatory-like process involving the development of cybersecurity standards and the creation of a "voluntary" program to encourage companies to follow these standards. Although the Executive Order does not create new legal obligations for companies, the Order could result in a federal agency responsible for a given sector issuing security requirements for companies within that sector.

Critical Infrastructure Defined

Potentially the most prominent question raised by companies considering the Executive Order is "who will be covered?" Because the ultimate goal of the Executive Order is the protection of the nation's "critical infrastructure," the definition of this term largely defines the Order's scope. In this regard, the term "critical infrastructure" is defined as the "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." While virtually all companies are subject to at least some cybersecurity risks, most companies likely do not maintain the types of systems and assets the destruction of which could lead to a "cyber Pearl Harbor," in the words of U.S. Defense Secretary Panetta.[3] Nonetheless, the definition provides limited practical guidance, particularly for large companies.

The responsibility to address the complex issue of what infrastructure is critical, at least with respect to infrastructure "at greatest risk," is left to the Secretary of DHS. Specifically, the Executive Order directs the Secretary of DHS, within 150 days, to conduct a risk-based assessment 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. If a company is identified as the owner and operator of such critical infrastructure, the Secretary of DHS, in coordination with the company's sector-specific agency, is directed to "confidentially notify" the company and provide the company with the basis for such determination. As a result, ultimately the federal government will decide who is "covered" and who is not. But many companies likely will not be viewed as owners and operators of "critical infrastructure."

Although critical infrastructure conceptually could be maintained in a wide spectrum of sectors, the Executive Order is largely focused on 16 specific sectors: (1) Chemical; (2) Commercial Facilities; (3) Communications;

[3] Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City (October 11, 2012), available here.

(4) Critical Manufacturing; (5) Dams; (6) Defense Industrial Base; (7) Emergency Services; (8) Energy; (9) Financial Services; (10) Food and Agriculture; (11) Government Facilities; (12) Healthcare and Public Health; (13) Information Technology; (14) Nuclear Reactors, Materials, and Waste; (15) Transportation Systems; and (16) Water and Wastewater Systems. For companies that do not operate in one of these sectors, the likelihood that DHS would identify that company as owning or operating critical infrastructure may be low.

Information Sharing

The issue of information sharing has been a critical one for the private sector throughout the current debate on cybersecurity. Specifically, the private sector has largely supported any effort that would improve the private sector's access to valuable cyber intelligence that the federal government obtains. For example, if the federal government knows of a specific cyber threat to a company, knowledge about that threat information may significantly assist the company in taking steps to prevent or mitigate the threat. Importantly, the Executive Order directs the Secretary of DHS, the Attorney General and the Director of National Intelligence to each issue instructions to ensure the timely production of declassified reports of cyber threats that identify a specific targeted entity. In turn, the Secretary of DHS and the Attorney General are directed to establish a process to rapidly disseminate declassified cyber threat reports to the targeted entity.

The concept of the federal government sharing cyber threat information with the private sector, however, has raised privacy and civil liberty concerns for some. Historically, the type of information shared between the private sector and the federal government has focused on cyber threat signatures and other technical information (e.g., the signature of a denial of service attack, which ports it is aimed at, where is it coming from, and how), and not personally identifiable information relating to individuals. Nonetheless, the Executive Order attempts to alleviate privacy concerns associated with the contemplated information sharing by directing the federal government to ensure that privacy and civil liberty protections based on the Fair Information Practice Principles are incorporated into its activities to implement the Order.

Security Clearances

Another critical issue for the private sector has been the availability of security clearances. Specifically, the private sector has supported efforts to improve private-sector access to security clearances to allow companies to receive critical classified cyber threat information. To address this point, the Executive Order directs the Secretary of DHS to expedite the processing of security clearances to appropriate personnel of owners and operators of critical infrastructure, with priority being provided to those companies notified by DHS that they maintain critical infrastructure. If properly effectuated, this aspect of the Executive Order should prove valuable for companies that own or operate critical infrastructure. But for those companies that do not own or operate critical infrastructure, access to security clearances may be unlikely, at least as a result of the Order.

The Cybersecurity Standards and the Voluntary Program

To assist companies in determining the actual security practices to employ to protect their critical infrastructure, the National Institute of Standards and Technology (NIST) will issue (and periodically update) a "Cybersecurity

Framework" that includes a set of standards, methodologies, procedures, and processes to address cyber risks.[4] This Framework will identify specific information security measures and controls to help owners and operators of critical infrastructure identify, assess and manage their cyber risks. Importantly, the Cybersecurity Framework is to be developed through "an open public review and comment process." Companies should have an opportunity to comment on the Framework and could potentially have a meaningful impact on the resulting standards.

In addition, the Secretary of DHS, in coordination with the sector-specific agencies, will encourage companies to implement the Cybersecurity Framework by establishing "a voluntary program to support the adoption of the" Framework ("Voluntary Program"). Because the President cannot directly impose legal obligations on companies, the Executive Order establishes the Voluntary Program to encourage (but not require) the adoption of the Cybersecurity Framework. Of course, this begs the question of why a company would elect to participate in the Program and agree to follow the security standards identified in the Framework. As a result, the Secretary of DHS is directed to establish "a set of incentives" that are designed to encourage companies to participate in this Voluntary Program and to make recommendations to the President as to whether these incentives can be provided under existing law or require new law. It is far from clear that DHS has the legal authority necessary to provide truly meaningful incentives to encourage participation in the Voluntary Program.

Adoption of the Cybersecurity Framework by Federal Agencies

Ultimately, companies in some sectors may find that the Cybersecurity Framework is not entirely "voluntary." For example, the Executive Order directs the various sector-specific agencies to review the Framework and, where necessary, develop implementation guidance or supplemental materials to address sector-specific risks. To the extent that a sector-specific agency does issue guidance, the guidance could apply broadly to companies within that sector, even potentially those that do not participate in the Voluntary Program or even those that do not own or operate covered critical infrastructure.

Also, the Executive Order directs executive-branch agencies that have responsibility for regulating the security of critical infrastructure to conduct risk assessments comparing existing regulatory requirements with the preliminary Framework issued by NIST.[5] Specifically, these agencies will be charged with determining if existing regulatory requirements are sufficient to address cybersecurity risk. If an agency determines that existing regulatory requirements are not sufficient, it must, within 90 days of the final Framework being issued, propose "prioritized, risk-based, efficient, and coordinated actions" to mitigate cyber risk. The phrase "prioritized, risk-based, efficient, and coordinated actions" is terribly vague. If an executive-branch agency finds that existing cybersecurity requirements for entities subject to its authority are insufficient and that agency also has statutory authority to issue regulations or guidance relating to cybersecurity, the agency may issue regulations. As a result, when the dust settles, some companies could find themselves with new regulatory requirements or guidance directing or expecting them to implement the types of security measures identified in the Cybersecurity Framework.

[4] The Executive Order includes an optimistic timeframe for the development of the Framework: 240 days for a preliminary version and one year for a final version.

[5] An Executive Order cannot direct an independent federal agency to act. Independent agencies include, for example, the Federal Reserve Board, the Federal Communications Commission, and the Bureau of Consumer Financial Protection. *See* 44 U.S.C. § 3502(5). Nonetheless, the Order "encourage[s]" these independent agencies to consider prioritized actions to mitigate cyber risks for critical infrastructure, consistent with their authorities.

THE EU DIRECTIVE

The draft EU Directive is designed to protect network and information systems ("NIS"), encourage information sharing among the EU Member States and protect critical infrastructure. As a result, the definition of companies that may be covered the EU Directive is substantially broader than that proposed by the Executive Order.[6] As currently drafted, the companies covered by the EU Directive would include:

(1) Providers of ***information society services***, including e-commerce platforms, Internet payment gateways, social networks, search engines, cloud service providers, and application stores; and

(2) Operators of ***critical infrastructure*** in the following sectors:

a. Energy (the non-exhaustive list refers to electricity and gas);

b. Transport (such as air and maritime carriers, railways, airports, ports, and auxiliary logistics services, including warehousing and storage, cargo handling, and other transportation support activities);

c. Banking (including savings and mortgage banks and electronic payment providers);

d. Stock exchanges; and

e. Health (including hospitals and private clinics and other health care providers).

The main obligations under the EU Directive would be for the covered entities to implement appropriate technical and organizational measures to minimize the risks to "network and information systems on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems."[7] This would include an obligation to notify the competent national regulator (to be designated by each Member State) about "incidents having a significant impact" on the continuity of the service. The national authority then may decide to notify the broader public when it deems that disclosure is in the public interest. In addition, the European Commission as well as the Member States may issue legislation to specify what security measures must be implemented, as well as how, when, and under what circumstances security incidents must be disclosed to the new national regulator.

New Regulatory Authorities and Goals

Each EU Member State would be obligated to adopt a NIS strategy that would include: (1) a risk assessment; (2) "general measures on preparedness, response and recovery;" (3) a strategy for sharing between the public and private sector; and (4) an education, training, and awareness program. Each Member State would be required to determine which authority within the country would be responsible for implementing and enforcing this EU Directive and to establish a Computer Emergency Response Team (CERT).[8] One key component of the

[6] The proposed EU Directive would not apply to public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services.

[7] The EU Directive would define a Network and Information System as an electronic communications network, a device used to perform automatic processing of computer data, or computer data. Computer data is not defined.

[8] Article 7 of the proposed EU Directive states that a "well-functioning" CERT must be established in each Member State under the supervision of the competent authority, to ensure effective capabilities to deal with cybersecurity incidents and ensure effective cooperation across the EU. Annex I to the EU Directive sets out detailed requirements for the CERT, which must be supported by national policy and/or legislation.

draft EU Directive would be to encourage cooperation among the EU Member State regulators and the CERTs that are to be established. Thus, the EU Directive calls for the appropriate authorities to regularly publish non-confidential information on early warnings on a common website, and share information regarding specific threats and responses to those threats.

Given that it is a proposed Directive (as opposed to a Regulation), each EU Member State would be obligated to implement the EU Directive into its own country's laws in order for it to have any effect on a company. At this stage, the EU Directive is simply a draft and must first be formally adopted at the EU level. Once adopted at the EU level, Member States will have 18 months to implement that EU Directive into national law. Thus, the earliest implementation of the rules likely would be January 2016.

PRACTICAL IMPLICATIONS

Many companies do not maintain the types of systems and assets that are deemed "critical infrastructure" for purposes of the Executive Order. Nonetheless, the U.S. government (and not companies themselves) will ultimately make the determination of which infrastructure is critical. It is inevitable that DHS will identify some companies as owning and operating critical infrastructure, even though those companies do not believe such identification is appropriate. No company wants to be caught off guard if this occurs. It is important that companies (particularly those in the 16 sectors identified in the Executive Order and the companies identified in the EU Directive) consider the scope and the extent to which new proposed rules may apply to them.

Moreover, even though the Executive Order and EU Directive do not directly create new legal obligations for companies, there are various ways in which the Order or Directive could result in new legal requirements being created. This is true even for companies that do not own or operate the type of infrastructure that is deemed critical. At a minimum, expectations regarding cybersecurity and preparedness will certainly be raised. It is critical that companies not focus on the "voluntary" or broad nature of the Executive Order and the EU Directive and work to improve their data security practices. Also, once the EU Directive is transposed into national law, these Member State laws will apply directly to companies,

While many of the time frames for implementation of the Executive Order are optimistic, it is important to keep in mind that NIST, DHS, and others have already begun their implementation activities. If the Order's deadlines are met, this year DHS will identify critical infrastructure "at greatest risk" and notify the companies that own and operate that infrastructure, and NIST will issue its preliminary Cybersecurity Framework. Particularly for those companies that believe there may be a risk that certain systems or assets maintained by them may be deemed critical, it is important to engage now. For example, these companies should consider the types of information security measures that may be appropriate in the Framework, any potential practical or technical issues raised by the Executive Order (including with respect to information sharing and the security clearance process), and the types of incentives that would meaningfully encourage participation in the Voluntary Program. When the opportunity arises to contribute to the implementation of the Executive Order, including through the public comment process associated with the development of the Framework, a company should be prepared to do so.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for nine straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law*," or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.