ALSTON&BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM FEBRUARY 13, 2013

White House Releases Executive Order Governing Critical Infrastructure

By Todd McClelland

Yesterday, the White House released an Executive Order titled "Improving Critical Infrastructure Cybersecurity" (the "Order"). The Order was signed by the President yesterday and announced during his State of the Union Address. The Order represents an attempt by the President to improve a perceived vulnerability to cyber attacks within the Nation's critical infrastructure.

The Order's stated purpose is 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." To achieve this purpose, the Order charges various governmental departments and agencies with, among other things, (i) increasing information sharing by requiring various agencies to report threats to specific targeted entities; (ii) developing a framework comprised of standards, methodologies, procedures and processes to reduce cyber risks to critical infrastructure (the "Framework"); (iii) evaluating the framework at the agency level against existing regulations and conducting a risk assessment to determine actions required to mitigate cyber risks and improve existing regulations; (iv) establishing a "voluntary program" to support the adoption of the framework by owners and operators of critical infrastructure; and (v) identifying and maintaining a list of especially high-risk critical infrastructure.

This cyber alert, presented in a "frequently asked questions" format, summarizes several key aspects of the Order.

Who is governed by the Order?

The Order applies to those entities that own or operate critical infrastructure, specifically, "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." This definition was borrowed and incorporated from the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c).

Does the Order apply to all Federal agencies?

No. The Order applies to any executive department (e.g., Department of Energy, Department of Commerce, Department of Homeland Security), military department, Government corporation, Government-controlled corporation or other establishment in the executive branch of the Government. It does not, however, apply to any independent regulatory agency, such as the Federal Reserve System, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Energy Regulatory Commission, the Securities and Exchange Commission, the Federal Trade Commission or the Nuclear Regulatory Commission.

What information sharing is required by the Order?

The Order represents a more specific mandate for cyber threat information sharing beyond that provided under Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, issued December 17, 2003, or its update issued in conjunction with the Order (PPD 21). The Order creates a more involved process obligating the intelligence community to share information about threats to "specific targeted entities." It appears to be the intent of the Order that if the U.S. intelligence community has unclassified information that a specific entity (a bank, perhaps) is the target of a cyber threat, that information will be shared with the entity. While governmental agencies have been notifying cyber attack targets for some time, the Order instructs several governmental entities, including the Director of National Intelligence, the Attorney General of the United States and the Secretary of Homeland Security to collaborate to establish a process for both the production of reports and the dissemination of those reports that identify specific targeted entities.

As an additional measure, the Order requires the Secretary of Homeland Security, in collaboration with the Secretary of Defense, to establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This program provides classified cyber threat and technical information to "eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure."

What is the Framework and how will it be developed?

The Order instructs the Secretary of Commerce to direct the National Institute of Standards and Technology (NIST) to coordinate the development of the Framework. This is familiar ground for NIST, which is responsible for developing standards and guidelines for information security for federal agencies pursuant to the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347. As defined by the Order, the Framework will be "a set of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks." The Order requires the incorporation of "voluntary consensus standards and industry best practices to the fullest extent possible," and is to be consistent with "voluntary international standards when such international standards will advance the objectives of this Order." The end result of this development process will be 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." The Framework is also required to include guidance for measuring an entity's performance in implementing the Framework. Importantly, the Framework is required to be technology-neutral, to enable technical innovation and account for organizational differences.

While the Framework may be a welcome development for those looking for a consolidation of the many standards used in industry, plaintiff lawyers and regulators may find fodder for future litigation and enforcement actions, especially for those organizations with low implementation measurements.

Will the Framework create new business regulations?

The Order charges agencies and departments (excluding independent regulatory agencies) to use the Framework as a comparison point for determining whether existing regulations are sufficient to defend against current and future anticipated risk. Agencies are required to begin the comparison process by consulting with the Department of Homeland Security, OMB and the National Security Staff to review the preliminary Framework to "determine if current cybersecurity regulatory requirements are sufficient given current and projected risks." Next, agencies are required to submit a report to the President that states whether or not the agency has "clear authority to establish requirements based upon the Framework to sufficiently address current and projected cyber risks to cyber infrastructure . . . ." If the agency does not have sufficient authority, the agency is required to propose "prioritized, risk-based, efficient, and coordinated actions . . . to mitigate cyber risk."

Based on this approach, the Order itself does not require agencies or departments to adopt the Framework, in whole or in part, as a part of their regulatory scheme. It is, however, intended to serve as a comparison point for assessing the adequacy of existing regulations. One should expect that where deficiencies are found in the required risk assessment, agencies will be

motivated to take regulatory action to resolve the gap. In addition, where regulations or applicable law fail to specify exact security measures (e.g., laws requiring "reasonable security"), the Framework may be used and cited for comparison purposes.

What programs is the government adopting to implement the Framework and is my company obligated to participate?

The Order outlines a process for the proposal of "incentives" to encourage owners and operators of critical infrastructure to join a voluntary program that supports the adoption of the Framework (the "Program"). The Order requires the Secretary of Homeland Security and the Secretaries of the Treasury Department and Commerce Department to develop such incentive proposals within 120 days of the date of the Order.

Of particular note for government and defense department contractors, the Order instructs the Secretary of Defense and the Administrator of General Services to make recommendations on the feasibility, security benefits and relative merits of incorporating security standards into acquisition planning and contract administration.

What is the importance of the "catastrophic" list and how will it be developed?

Within 150 days of the date of the Order, and annually thereafter, the Secretary of Homeland Security, in consultation with sector-specific agencies and other identified parties, is 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." This list is to be provided to the President and in confidence to the owners and operators of the identified critical infrastructure. Notified owners and operators are to be provided the basis for the determination and may request reconsideration through a process to be established by the Secretary.

The Order requires agencies considering changes to their regulations (discussed above) to take into account entities identified by this process. Otherwise, the Order provides no other discussion of the impact of being identified by the Secretary.

An obvious question one must consider is if an owner or operator is so notified, is any particular action required by that entity? When read in connection with other laws, such as laws governing the disclosure of material risks under the U.S. Securities Exchange Commission, identification on this list could give rise to potential disclosure obligations. Also, laws requiring "reasonable security" could call for an increase both in risk assessment and measures implemented to secure against cyber threats. There are likely many more implications with being identified. Finally, while the list appears to be a confidential document, any public disclosure of the document potentially causes a heightened risk to those identified entities.

Conclusion

The foregoing is a summary of certain key aspects of the Order. The Order has other elements and requirements that also deserve attention, such as the required consultation among agencies and key industry stakeholders. The Order also attempts to balance the desired security efforts against protecting privacy and civil liberties.

Alston & Bird has a team of lawyers and public policy experts who have been and will continue to follow developments with this Order. Please feel free to contact any of the lawyers identified below if you have any questions.

James A. Harvey | 404.881.7328 | jim.harvey@alston.com

Todd S. McClelland | 404.881.4789 | todd.mcclelland@alston.com

Kimberly K. Peretti | 202.239.3720 | kimberly.peretti@alston.com