SUMMARY OF EXECUTIVE ORDER ON IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Overview

Identification of Critical Infrastructure. Not later than July 12, 2013, the Secretary of Homeland Security is directed to identify critical infrastructure where a cybersecurity incident could result in catastrophic regional or national effects on public health or safety, economic security, or national security, using a consultative process and drawing on the expertise of the Sector Specific Agencies (SSAs) designated in the Presidential Directive that accompanied the release of the Executive Order. The Department of Homeland Security (DHS) is the SSA for communications. The owners and operators of such critical infrastructure will be notified confidentially and will be permitted to submit relevant information and request reconsideration of the Secretary's determination.

IT Carve-out. The Order prohibits the Secretary from identifying any commercial information technology products or consumer information technology services.

Cybersecurity Framework. The National Institute of Standards and Technology (NIST) will lead the development of a Cybersecurity Framework relying, to the fullest extent possible, on existing consensus-based standards and guidelines. The framework must provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. NIST must publish a preliminary version of the Framework by October 10, 2013, and a final version by February 12, 2014. NIST has already released a pre-publication version of its RFI to gather information for developing the Framework. Interested parties will have 45 days to comment once the RFI is published in the Federal Register.

Agency Review. The preliminary Cybersecurity Framework must be reviewed for sufficiency by all Executive Branch agencies with responsibility for regulating the security of critical infrastructure. Not later than January 8, 2014, these agencies must submit a report to the President on whether or not the agency has clear authority to establish requirements based on the framework. As an independent regulatory agency, the Federal Communications Commission is not required to take part in the review, but the Order encourages independent regulatory agencies with responsibility for the security of critical infrastructure to take part in a consultative process to consider prioritized actions to mitigate cyber risks.

Voluntary Adoption of Framework. The DHS Secretary, in coordination with SSAs, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure, and shall coordinate establishment of a set of incentives to promote participation in the program. Not later than June 12, 2013, the Secretaries of Homeland Security, Commerce, and Treasury must each review the incentives and make recommendations on their effectiveness, and on whether new legislation may be required to implement the incentives.

Information Sharing. By June 12, 2013, the DHS Secretary, Attorney General, and Director of National Intelligence shall issue instructions to ensure the timely production of unclassified reports of cyber threats to U.S. private sector entities in a timely manner. Also by June 12, 2013, the DHS Secretary shall establish procedures to expand the voluntary Enhanced Cybersecurity Services program to allow the Federal Government to share classified cyber threat and technical information to eligible entities in all critical infrastructure sectors.

A more detailed summary follows below.

Summary

Policy

The Order announces the policy of the United States 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.

Definition of Critical Infrastructure

Critical Infrastructure is defined to mean systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or a combination thereof. This is the same definition contained in the Homeland Security Act.

Cybersecurity Information Sharing

The Order directs the Attorney General, the Secretary of Homeland Security ("Secretary"), and the Director of National Intelligence to issue instructions to ensure the timely production of unclassified reports of cyber threats that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall also establish a process for the rapid dissemination of these reports to the targeted entity.

Within 120 days of the date of the Order, the Secretary shall, in collaboration with the Secretary of Defense, establish procedures to expand the Enhanced Cybersecurity Services program, a voluntary information sharing program that provides classified cyber threat and technical information from the Government to eligible critical infrastructure companies and those that provide security services to critical infrastructure, to all critical infrastructure sectors.

Privacy and Civil Liberties Protections

Executive Branch agencies shall coordinate activities under this order with their senior agency officials for privacy and civil liberties to ensure that protections based upon the Fair Information Practice Principles (notice, consent, etc.) and other privacy and civil liberties policies are

incorporated into such activities. Not later than February 12, 2014, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties at DHS shall release a report on ways to minimize the privacy and civil liberties risks of the activities undertaken by DHS under this Order. The report shall be reviewed on an annual basis and revised as necessary.

Consultative Process

The Secretary shall engage and consider the advice of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector Specific Agencies; State, local, territorial and tribal governments; universities; and outside experts to establish a consultative process to coordinate improvements to critical infrastructure cybersecurity.

Baseline Framework to Reduce Cyber Risk to Critical Infrastructure

The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology to lead the development of a framework to reduce cyber risks to critical infrastructure that will include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. To develop this Cybersecurity Framework, the Director shall engage in an open review and comment process, and shall consult with other Federal departments and agencies, owners and operators of critical infrastructure, and other stakeholders. A preliminary version of the framework shall be published within 240 days of the date of the Order.

To the extent possible, the framework shall incorporate voluntary consensus standards and industry best practices and shall be consistent with voluntary international standards. The framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The framework shall: identify cross-sector security standards and guidelines; identify areas for improvement; be technology neutral; include guidance for measuring implementation performance; and include methodologies to mitigate the impact of the framework on business confidentiality and to protect privacy and civil liberties.

Voluntary Critical Infrastructure Cybersecurity Program

The Secretary, in coordination with the SSAs, shall establish a voluntary Cybersecurity Program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure. The SSAs shall coordinate with the Sector Coordinating Councils to develop implementation guidance or supplemental materials to address sector-specific risks and operative environments. The SSAs shall report annually on the extent to which owners and operators are participating in the Program.

The Secretary shall coordinate the establishment of a set of incentives designed to promote participation in the program. Within 120 days of the date of the Order, the Secretaries of Homeland Security, Commerce, and the Treasury shall separately make recommendations to the

effectiveness of such incentives, and whether the incentives can be provided under existing law or would require new legislation.

Within 120 days of the date of the Order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisitions Regulatory Council, shall make recommendations to the President on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration.

Identification of Critical Infrastructure at Greatest Risk

Within 150 days of the date of the Order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic effects on public health or safety, economic security, or national security. The Secretary shall use the consultative process established by this Order and shall apply consistent objective criteria in identifying critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services. The Secretary shall annually review and update this list of identified critical infrastructure.

In coordination with SSAs, the Secretary shall confidentially notify owners and operators of critical infrastructure identified on the list and shall provide the basis of the determination to those owners and operators. The Secretary shall establish a process by which the owners and operators of identified critical infrastructure may submit relevant information and request reconsideration.

Adoption of Framework

Executive Branch agencies with responsibility for regulating the security of critical infrastructure shall engage in the consultative process to review the preliminary Cybersecurity Framework to determine their sufficiency. These agencies shall submit a report to the President that states whether or not the agency has clear authority to establish requirements based on the Cybersecurity Framework to sufficiently address current and projected cyber risks.

If current regulatory requirements are deemed insufficient, the agencies shall propose, within 90 days of the date of the Order, prioritized, risk-based, efficient, and coordinated actions to mitigate cyber risks. Within two years after publication of the final Framework, the appropriate agencies, in consultation with owners and operators of critical infrastructure, shall report to the Office of Management and Budget on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements.

Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in the consultative process.