EXECUTIVE ORDER

---

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the Authority vested in me as President by the Constitution and laws of the United States of America, it is hereby ordered as follows:

Sec. 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the protection 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. We will achieve these goals through a partnership with the owners and operators of critical infrastructure that includes cybersecurity information sharing and the collaborative development and the adoption of risk-based standards.

Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure has the meaning given in 42 U.S.C. 5195c(e). For purposes of this order, a product or service used by critical infrastructure shall not be considered to be critical infrastructure unless the product or service meets the definition in 42 U.S.C. 5195c(e).

Sec. 3. Policy Coordination. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive-1 of February 13, 2009 (Organization of the National Security Council System).

Sec. 4. Cybersecurity Information Sharing. (a) Within 120 days of the date of this order, the Director of National Intelligence shall issue instructions to the intelligence community consistent with 50 U.S.C. 403-1(i), and the Attorney General of the United States shall issue instructions consistent with 42 U.S.C. 10607(b) to federal law enforcement entities under the Attorney General's authority, to ensure the timely production of unclassified versions of all reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The Secretary of Homeland Security (the Secretary) shall produce timely unclassified versions of all Department of Homeland Security reports of cyber threats to the U.S. homeland that identify a specific targeted entity.

(b) The Secretary, consistent with 6 U.S.C. 133(g), shall establish a coordinated process that rapidly disseminates all unclassified reports of cyber threats that identify a specific targeted entity to the U.S. targeted entity. The Secretary, in coordination with the Director of National

Intelligence, shall establish a system for the tracking of these reports and notifications. Agencies making notifications are responsible for reporting to the Secretary when notifications are made.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of Defense, shall within 120 days of the date of this order establish procedures to allow the owners and operators of critical infrastructure in all sectors to participate, on a voluntary basis, in the Enhanced Cybersecurity Services initiative.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the provision of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Sec. 5. Privacy and Civil Liberties Protections. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities based upon the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles and frameworks.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security shall assess the privacy and civil liberties risks of the functions and programs called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within one year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to the Department of Homeland Security for consideration and inclusion in the report. The report shall be reviewed and revised as necessary on an annual basis thereafter. The report may contain a classified annex if necessary. Assessments will include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles and frameworks.

(c) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security shall coordinate the report required under subsection (b) of this section with the Office of Management and Budget (OMB) and the Privacy and Civil Liberties Oversight Board.

(d) Agencies shall consider the assessments and recommendations of the report, and, in coordination with their senior privacy and civil liberties officials, shall include privacy and civil liberties protections in agency activities.

(e) Information submitted voluntarily by private entities under this order, in accordance with 6 U.S.C. 133, shall be protected from disclosure to the fullest extent permitted by law.

Sec. 6. Consultative Process. The Secretary shall establish a consultative process using the Critical Infrastructure Partnership Advisory Council (CIPAC), to coordinate improvements to the cybersecurity of critical infrastructure. The Secretary shall facilitate the engagement and consider advice on matters set forth in this order of the Sector Coordinating Councils, critical infrastructure owners and operators, Sector-Specific Agencies, other relevant agencies, independent regulatory agencies, state, local, territorial, and tribal governments, universities, and outside experts.

Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the Director) to coordinate the development of a framework to reduce cyber risks to critical infrastructure (the Cybersecurity Framework). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate existing consensus-based standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with international standards whenever feasible, and shall meet the requirements of the National Institute of Standards and Technology Act, Public Law 104-113, and OMB Circular A-119.

(b) The Cybersecurity Framework shall 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. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Framework will also identify potential gaps that should be addressed through collaboration with particular sectors and industry-led standards organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide cybersecurity 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. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) Within 240 days of the date of this order, and after completion of the consultation process required under subsection (d) of this section, the Director shall publish a preliminary version of the Cybersecurity Framework (the preliminary Framework). Within one year of the date of this

order, and after review by the Secretary, the Director shall publish a final version of the Cybersecurity Framework (the final Framework).

(e) In coordinating development of the preliminary and final Cybersecurity Framework, as well as any updates, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, Sector-Specific Agencies and other interested agencies, OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information, including unclassified reports relating to cyber threats, and technical expertise, to inform the Cybersecurity Framework and the consultative development process.

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, in consultation with the Secretary, Sector-Specific Agencies and other interested agencies, OMB, owners and operators of critical infrastructure, and other stakeholders, at least every 3 years, taking into consideration changes in cyber risks, operational feedback from owners and operator of critical infrastructure and any other relevant factors.

Sec.8. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the Program).

(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 90 days of the date of this order, the Secretary and the Secretaries of Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on what incentives can be provided to owners and operators of critical infrastructure that participate in the Program, under existing law and authorities, and what incentives would require legislation, including analysis of the benefits and relative effectiveness of such incentives.

(e) Within 90 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and

relative merits of changing the federal procurement process to create preferences for vendors who meet cybersecurity standards, and to harmonize and make consistent existing procurement requirements related to cybersecurity. In developing such recommendations, the Secretary of Defense and the Administrator of General Services shall consult with the Federal Acquisition Regulatory Council and shall use the consultative process established in section 6 of this order.

Sec. 9. Identification of Critical Infrastructure at Greatest Risk. (a) Within 150 days of the date of this order, consistent with 6 U.S.C. 124*l*, the Secretary shall use a risk-based approach 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. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in making such identifications. The Secretary shall not identify any commercial information technology products under this section. The Secretary shall review and update identifications under this section on an annual basis, and provide each such identification to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided with relevant threat information. The Secretary shall establish a process through which notified owners and operators of critical infrastructure may submit relevant information and request reconsideration of an identification under subsection (a)of this section.

Sec. 10. Adoption by Agencies. (a) Agencies, as defined under section 11(a) of this order (not including independent regulatory agencies) with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with the Department of Homeland Security, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, agencies shall consider the identification of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director ofOMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, any additional authority required, and the extent to which existing requirements overlap, conflict, or could be harmonized.

(b) If current regulatory requirements are deemed to be insufficient, within 60 days of publication of the final Framework, agencies shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), and Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), to mitigate cyber risk. All agencies shall seek to harmonize cybersecurity requirements across sectors through the use of the Cybersecurity Framework, adding to it as necessary to suit the specific needs of the agency's sector.

(c) Within two years after publication of the final Framework, agencies shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to duplicative, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary and affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with each independent regulatory agency's authorities.

Sec. 11. Definitions. (a) "Agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) "Critical Infrastructure Partnership Advisory Council" means the council established by the Department of Homeland Security under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government, the private sector, and State, local, territorial, and tribal governments.

(c) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace and in the Framework for Privacy Policy at the Department of Homeland Security.

(d) "Independent regulatory agency" has the meaning given the term in 44 U.S.C. 3502(5).

(e) "Sector Coordinating Council" means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or its successor.

(f) "Sector-Specific Agency" has the meaning given the term in Homeland Security Presidential Directive 7 of December 17, 2003 (Critical Infrastructure Identification, Prioritization, and Protection), or its successor.

Sec. 12. General Provisions. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e ) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,