Executive Order -- Promoting Private Sector Cybersecurity Information Sharing

EXECUTIVE ORDER

- - - - - - -

PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION SHARING

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

Section 1. Policy. In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.

Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States.

This order builds upon the foundation established by Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), and Presidential Policy Directive-21 (PPD-21) of February 12, 2013 (Critical Infrastructure Security and Resilience).

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-l (PPD-l) of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 2. Information Sharing and Analysis Organizations. (a) The Secretary of Homeland Security (Secretary) shall strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs).

(b) ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.

(c) The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002 (the "Act"), shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information

related to cybersecurity risks and incidents, addressing such risks and incidents, and strengthening information security systems consistent with sections 212 and 226 of the Act.

(d) In promoting the formation of ISAOs, the Secretary shall consult with other Federal entities responsible for conducting cybersecurity activities, including Sector-Specific Agencies, independent regulatory agencies at their discretion, and national security and law enforcement agencies.

Sec. 3. ISAO Standards Organization. (a) The Secretary, in consultation with other Federal entities responsible for conducting cybersecurity and related activities, shall, through an open and competitive process, enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization (SO), which shall identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs under this order. The standards shall further the goal of creating robust information sharing related to cybersecurity risks and incidents with ISAOs and among ISAOs to create deeper and broader networks of information sharing nationally, and to foster the development and adoption of automated mechanisms for the sharing of information. The standards will address the baseline capabilities that ISAOs under this order should possess and be able to demonstrate. These standards shall address, but not be limited to, contractual agreements, business processes, operating procedures, technical means, and privacy protections, such as minimization, for ISAO operation and ISAO member participation.

(b) To be selected, the SO must demonstrate the ability to engage and work across the broad community of organizations engaged in sharing information related to cybersecurity risks and incidents, including ISAOs, and associations and private companies engaged in information sharing in support of their customers.

(c) The agreement referenced in section 3(a) shall require that the SO engage in an open public review and comment process for the development of the standards referenced above, soliciting the viewpoints of existing entities engaged in sharing information related to cybersecurity risks and incidents, owners and operators of critical infrastructure, relevant agencies, and other public and private sector stakeholders.

(d) The Secretary shall support the development of these standards and, in carrying out the requirements set forth in this section, shall consult with the Office of Management and Budget, the National Institute of Standards and Technology in the Department of Commerce, Department of Justice, the Information Security Oversight Office in the National Archives and Records Administration, the Office of the Director of National Intelligence, Sector-Specific Agencies, and other interested Federal entities. All standards shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.

Sec. 4. Critical Infrastructure Protection Program. (a) Pursuant to sections 213 and 214(h) of the Critical Infrastructure Information Act of 2002, I hereby designate the NCCIC as a critical infrastructure protection program and delegate to it authority to enter into voluntary agreements with ISAOs in order to promote critical infrastructure security with respect to cybersecurity.

(b) Other Federal entities responsible for conducting cybersecurity and related activities to address threats to the public health and safety, national security, and economic security, consistent with the objectives of this order, may participate in activities under these agreements.

(c) The Secretary will determine the eligibility of ISAOs and their members for any necessary facility or personnel security clearances associated with voluntary agreements in accordance with Executive Order 13549 of August 18, 2010 (Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities), and Executive Order 12829 of January 6, 1993 (National Industrial Security Program), as amended, including as amended by this order.

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 appropriate protections for privacy and civil liberties are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) Senior privacy and civil liberties officials for agencies engaged in activities under this order shall conduct assessments of their agency's activities and provide those assessments to the Department of Homeland Security (DHS) Chief Privacy Officer and the DHS Office for Civil Rights and Civil Liberties for consideration and inclusion in the Privacy and Civil Liberties Assessment report required under Executive Order 13636.

Sec. 6. National Industrial Security Program. Executive Order 12829, as amended, is hereby further amended as follows:

(a) the second paragraph is amended by inserting "the Intelligence Reform and Terrorism Prevention Act of 2004," after "the National Security Act of 1947, as amended,";

(b) Sec. 101(b) is amended to read as follows: "The National Industrial Security Program shall provide for the protection of information classified pursuant to Executive Order 13526 of December 29, 2009, or any predecessor or successor order, and the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 *et seq.*).";

(c) Sec. 102(b) is amended by replacing the first paragraph with: "In consultation with the National Security Advisor, the Director of the Information Security Oversight Office, in accordance with Executive Order 13526 of December 29, 2009, shall be responsible for implementing and monitoring the National Industrial Security Program and shall:";

(d) Sec. 102(c) is amended to read as follows: "Nothing in this order shall be construed to supersede the authority of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 *et seq.*), or the authority of the Director of National Intelligence (or any Intelligence Community element) under the Intelligence Reform and Terrorism Prevention Act of 2004, the National Security Act of 1947, as amended, or Executive Order 12333 of December 8, 1981, as amended, or the authority of the Secretary of Homeland Security, as the Executive Agent for the Classified National Security Information Program established under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities).";

(e) Sec. 201(a) is amended to read as follows: "The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Nuclear Regulatory Commission, the Director of National Intelligence, and the Secretary of Homeland Security, shall issue and maintain a National Industrial Security Program Operating Manual (Manual). The Secretary of Energy and the Nuclear Regulatory Commission shall prescribe and issue that portion of the Manual that pertains to information classified under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 *et seq.*). The Director of National Intelligence shall

prescribe and issue that portion of the Manual that pertains to intelligence sources and methods, including Sensitive Compartmented Information. The Secretary of Homeland Security shall prescribe and issue that portion of the Manual that pertains to classified information shared under a designated critical infrastructure protection program.";

(f) Sec. 201(f) is deleted in its entirety;

(g) Sec. 201(e) is redesignated Sec. 201(f) and revised by substituting "Executive Order 13526 of December 29, 2009, or any successor order," for "Executive Order No. 12356 of April 2, 1982.";

(h) Sec. 201(d) is redesignated Sec. 201(e) and revised by substituting "the Director of National Intelligence, and the Secretary of Homeland Security" for "and the Director of Central Intelligence.";

(i) a new Sec. 201(d) is inserted after Sec. 201(c) to read as follows: "The Manual shall also prescribe arrangements necessary to permit and enable secure sharing of classified information under a designated critical infrastructure protection program to such authorized individuals and organizations as determined by the Secretary of Homeland Security.";

(j) Sec. 202(b) is amended to read as follows: "The Director of National Intelligence retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information. The Director of National Intelligence may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information or may enter into written agreements with the Secretary of Defense, as Executive Agent, or with the Director of the Central Intelligence Agency to inspect and monitor these programs or facilities, in whole or in part, on the Director's behalf.";

(k) Sec. 202(d) is redesignated as Sec. 202(e); and

(l) in Sec. 202 a new subsection (d) is inserted after subsection (c) to read as follows: "The Secretary of Homeland Security may determine the eligibility for access to Classified National Security Information of contractors, licensees, and grantees and their respective employees under a designated critical infrastructure protection program, including parties to agreements with such program; the Secretary of Homeland Security may inspect and monitor contractor, licensee, and grantee programs and facilities or may enter into written agreements with the Secretary of Defense, as Executive Agent, or with the Director of the Central Intelligence Agency, to inspect and monitor these programs or facilities in whole or in part, on behalf of the Secretary of Homeland Security."

Sec. 7. Definitions. (a) "Critical infrastructure information" has the meaning given the term in section 212(3) of the Critical Infrastructure Information Act of 2002.

(b) "Critical infrastructure protection program" has the meaning given the term in section 212(4) of the Critical Infrastructure Information Act of 2002.

(c) "Cybersecurity risk" has the meaning given the term in section 226(a)(1) of the Homeland Security Act of 2002 (as amended by the National Cybersecurity Protection Act of 2014).

(d) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(e) "Incident" has the meaning given the term in section 226(a)(2) of the Homeland Security Act of 2002 (as amended by the National Cybersecurity Protection Act of 2014).

(f) "Information Sharing and Analysis Organization" has the meaning given the term in section 212(5) of the Critical Infrastrucure Information Act of 2002.

(g) "Sector-Specific Agency" has the meaning given the term in PPD-21, or any successor.

Sec. 8. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law or Executive Order to an agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law including those activities conducted with the private sector relating to criminal and national security threats. 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.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods.

(d) 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.

BARACK OBAMA