EXECUTIVE ORDER

13718

- - - - - - -

COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to enhance cybersecurity awareness and protections at all levels of Government, business, and society, to protect privacy, to ensure public safety and economic and national security, and to empower Americans to take better control of their digital security, it is hereby ordered as follows:

Section 1. Establishment. There is established within the Department of Commerce the Commission on Enhancing National Cybersecurity (Commission).

Sec. 2. Membership. (a) The Commission shall be composed of not more than 12 members appointed by the President. The members of the Commission may include those with knowledge about or experience in cybersecurity, the digital economy, national security and law enforcement, corporate governance, risk management, information technology (IT), privacy, identity management, Internet governance and standards, government administration, digital and social media, communications, or any other area determined by the President to be of value to the Commission. The Speaker of the House of Representatives, the Minority Leader of the House of Representatives, the Majority Leader of the Senate, and the Minority Leader of the Senate are each invited to recommend one individual for membership on the Commission. No federally registered lobbyist or person presently otherwise employed by the Federal Government may serve on the Commission.

(b) The President shall designate one member of the Commission to serve as the Chair and one member of the Commission to serve as the Vice Chair.

Sec. 3. Mission and Work. The Commission will make detailed recommendations to strengthen cybersecurity in both the public and private sectors while protecting privacy, ensuring public safety and economic and national security, fostering discovery and development of new technical solutions, and bolstering partnerships between Federal, State, and local government and the private sector in the development, promotion, and use of cybersecurity technologies, policies, and best practices. The Commission's recommendations should address actions that can be taken over the next decade to accomplish these goals.

(a) In developing its recommendations, the Commission shall identify and study actions necessary to further improve cybersecurity awareness, risk management, and adoption of best practices throughout the private sector and at all levels of government. These areas of study may include methods to influence the way individuals and organizations perceive and use technology and approach cybersecurity as consumers and providers in the digital economy; demonstrate the nature and severity of cybersecurity threats, the importance of mitigation, and potential ways to manage and reduce the economic impacts of cyber risk; improve access to the knowledge needed to make informed cyber risk management decisions related to privacy, economic impact, and business continuity; and develop partnerships with industry, civil society, and international stakeholders. At a minimum, the Commission shall develop recommendations regarding:

(i) how best to bolster the protection of systems and data, including how to advance identity

management, authentication, and cybersecurity of online identities, in light of technological developments and other trends;

(ii) ensuring that cybersecurity is a core element of the technologies associated with the Internet of Things and cloud computing, and that the policy and legal foundation for cybersecurity in the context of the Internet of Things is stable and adaptable;

(iii) further investments in research and development initiatives that can enhance cybersecurity;

(iv) increasing the quality, quantity, and level of expertise of the cybersecurity workforce in the Federal Government and private sector, including through education and training;

(v) improving broad-based education of commonsense cybersecurity practices for the general public; and

(vi) any other issues that the President, through the Secretary of Commerce (Secretary), requests the Commission to consider.

(b) In developing its recommendations, the Commission shall also identify and study advances in technology, management, and IT service delivery that should be developed, widely adopted, or further tested throughout the private sector and at all levels of government, and in particular in the Federal Government and by critical infrastructure owners and operators. These areas of study may include cybersecurity technologies and other advances that are responsive to the rapidly evolving digital economy, and approaches to accelerating the introduction and use of emerging methods designed to enhance early detection, mitigation, and management of cyber risk in the security and privacy, and business and governance sectors. At a

minimum, the Commission shall develop recommendations regarding:

(i) governance, procurement, and management processes for Federal civilian IT systems, applications, services, and infrastructure, including the following:

(A) a framework for identifying which IT services should be developed internally or shared across agencies, and for specific investment priorities for all such IT services;

(B) a framework to ensure that as Federal civilian agencies procure, modernize, or upgrade their IT systems, cybersecurity is incorporated into the process;

(C) a governance model for managing cybersecurity risk, enhancing resilience, and ensuring appropriate incident response and recovery in the operations of, and delivery of goods and services by, the Federal Government; and

(D) strategies to overcome barriers that make it difficult for the Federal Government to adopt and keep pace with industry best practices;

(ii) effective private sector and government approaches to critical infrastructure protection in light of current and projected trends in cybersecurity threats and the connected nature of the United States economy;

(iii) steps State and local governments can take to enhance cybersecurity, and how the Federal Government can best support such steps; and

(iv) any other issues that the President, through the Secretary, requests the Commission to consider.

(c) To accomplish its mission, the Commission shall:

(i) reference and, as appropriate, build on successful existing cybersecurity policies, public-private partnerships, and other initiatives;

(ii) consult with cybersecurity, national security and law enforcement, privacy, management, technology, and digital economy experts in the public and private sectors;

(iii) seek input from those who have experienced significant cybersecurity incidents to understand lessons learned from these experiences, including identifying any barriers to awareness, risk management, and investment;

(iv) review reported information from the Office of Management and Budget regarding Federal information and information systems, including legacy systems, in order to assess critical Federal civilian IT infrastructures, governance, and management processes;

(v) review the impact of technological trends and market forces on existing cybersecurity policies and practices; and

(vi) examine other issues related to the Commission's mission that the Chair and Vice Chair agree are necessary and appropriate to the Commission's work.

(d) Where appropriate, the Commission may conduct original research, commission studies, and hold hearings to further examine particular issues.

(e) The Commission shall be advisory in nature and shall submit a final report to the President by December 1, 2016.

This report shall be published on a public website along with any appropriate response from the President within 45 days after it is provided to the President.

Sec. 4. Administration. (a) The Commission shall hold periodic meetings in public forums in an open and transparent environment.

(b) In carrying out its mission, the Commission shall be informed by, and shall strive to avoid duplicating, the efforts of other governmental entities.

(c) The Commission shall have a staff, headed by an Executive Director, which shall provide support for the functions of the Commission. The Secretary shall appoint the Executive Director, who shall be a full-time Federal employee, and the Commission's staff. The Executive Director may also serve as the Designated Federal Officer in accordance with the Federal Advisory Committee Act, as amended, 5 U.S.C. App. (FACA, the "Act").

(d) The Executive Director, in consultation with the Chair and Vice Chair, shall have the authority to create subcommittees as necessary to support the Commission's work and to examine particular areas of importance. These subcommittees must report their work to the Commission to inform its final recommendations.

(e) The Secretary will work with the heads of executive departments and agencies, to the extent permitted by law and consistent with their ongoing activities, to provide the Commission such information and cooperation as it may require for purposes of carrying out its mission.

Sec. 5. Termination. The Commission shall terminate within 15 days after it presents its final report to the President, unless extended by the President.

Sec. 6. General Provisions. (a) To the extent permitted by law, and subject to the availability of appropriations, the Secretary shall direct the Director of the National Institute of Standards and Technology to provide the Commission with such expertise, services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission.

(b) Insofar as FACA may apply to the Commission, any functions of the President under that Act, except for those in section 6 and section 14 of that Act, shall be performed by the Secretary.

(c) Members of the Commission shall serve without any compensation for their work on the Commission, but shall be allowed travel expenses, including per diem in lieu of subsistence, to the extent permitted by law for persons serving intermittently in the Government service (5 U.S.C. 5701-5707).

(d) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to a department, 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.

(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,

February 9, 2016.

[FR Doc. 2016-03038 Filed: 2/11/2016 8:45 am; Publication Date: 2/12/2016]