U.S DEPARTMENT OF COMMERCE
COMMISSION ON ENHANCING NATIONAL CYBERSECURITY
CHARTER

1. Committee's Official Designation. Commission on Enhancing National Cybersecurity (the "Commission").

2. Authority. The Commission on Enhancing National Cybersecurity is being established pursuant to Executive Order 13718 dated February 9, 2016, in accordance with the provisions of the Federal Advisory Committee Act (FACA), 5 U.S.C. App., as amended.

3. Objectives and Scope of Activities. 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.

In developing its recommendations the Commission will identify and study actions necessary to further improve cybersecurity awareness, risk management, and the adoption of best practices throughout the private sector and at all levels of government. These areas of study may include methods to (a) influence the way individuals and organizations perceive and use technology and approach cybersecurity as consumers and providers in the digital economy; (b) 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; (c) improve access to the knowledge needed to make informed cyber risk management decisions related to privacy, economic impact, and business continuity; and (d) develop partnerships with industry, civil society, and international stakeholders.

In developing its recommendations, the Commission will 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.

4. Description of Duties. The functions of the Commission are advisory only. At a minimum, the Commission shall develop recommendations regarding:

(a) 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; 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; further investments in research and development initiatives that can enhance cybersecurity; increasing the quality, quantity, and level of expertise of the cybersecurity workforce in the Federal Government and private sector, including through education and training; improving broad-based education of commonsense cybersecurity practices for the general public; and any other issues that the President, through the Secretary, requests the Commission to consider; and

(b) governance, procurement, and management processes for Federal civilian IT systems, applications, services, and infrastructure, including the following: (1) 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; (2) a framework to ensure that as Federal civilian agencies procure, modernize, or upgrade their IT systems, cybersecurity is incorporated into the process; (3) 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 (4) strategies to overcome barriers that make it difficult for the Federal Government to adopt and keep pace with industry best practices; 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; steps State and local governments can take to enhance cybersecurity, and how the Federal Government can best support such steps; and any other issues that the President, through the Secretary, requests the Commission to consider.

To accomplish its objectives and activities, the Commission shall:

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

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

(c) 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;

(d) 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 information technology infrastructures, governance, and management processes;

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

(f) 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.

Where appropriate and subject to the availability of funds, the Commission may conduct original research, commission studies, and hold hearings to further examine particular issues. The Commission will submit a final report to the President. The report will be published on a public website along with any appropriate response from the President within 45 days after it is provided to the President.

5. Agency or Official to Whom the Committee Reports. The Commission is established within the Department of Commerce and reports to the President.

Presidential Advisory Committee Follow-up Report: DOC is responsible for ensuring the reporting requirements of Section 6(b) of FACA are fulfilled.

6. Support. The Commission shall have a staff, headed by an Executive Director, which shall provide support for the functions of the Commission. The Secretary of Commerce (the Secretary) shall appoint the Executive Director, who shall be a full-time Federal employee, and the Commission's staff.

7. Estimated Annual Operating Costs and Staff Years. The estimated cost for operating the Commission is $5.5M. Operating costs include 6 full-time equivalent staff; contract resources to provide the Commission with technical research, documentation, and logistics support; support for multiple public meetings and related technical capabilities (e.g., webcasting); travel expenses for Commission and federal staff; and other operating expenses necessary to meet the short term objectives of the Commission. Members shall serve without compensation for their work on the Commission, but shall be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law, consistent with the availability of funds.

8. Designated Federal Officer. The Executive Director shall serve as the Designated Federal Officer (DFO), in accordance with FACA. The DFO will (a) approve or call the meeting of the Commission or any subcommittee; (b) attend the meetings; (c) adjourn any meeting when he or she determines it to be in the public interest; and (d) chair the meeting when so directed by the agency head.

9. Estimated Number and Frequency of Meetings. It is expected that the Commission will meet approximately once a month. The DFO shall ensure the meetings comply with the requirements of FACA and its implementing regulations. Commission meetings shall be open to the public unless closed per a stipulation in the Government and Sunshine Act and consistent with FACA requirements.

10. Duration. Executive Order 13718 requires the Commission to submit its final report to the President by December 1, 2016.

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

12. Membership and Designation. 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 have each been 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. 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.

Commission members serve from appointment until the termination of the Commission, at the pleasure of the President. If the Commission is extended, members may be reappointed to any number of additional terms, provided that the member proves to work effectively on the Commission and his/her knowledge and advice are still needed.

13. Subcommittees 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.

14. Recordkeeping. Records of the Commission and the respective subcommittees or subgroups shall be handled in accordance with General Records Schedule 6.2 or other approved agency records disposition schedule. These records shall be available for public inspection and copying, subject to the Freedom of Information Act, 5 U.S.C. 552.

Ellen Herbst
Chief Financial Officer and
Assistant Secretary for Administration

3/25/16
Filing Date