Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket Number: 160725650-6650-01

Information on Current and Future States of Cybersecurity in the Digital Economy

AGENCY: National Institute of Standards and Technology, U.S. Department of Commerce.

ACTION: Notice; Request for Information (RFI).

SUMMARY: The Commission on Enhancing National Cybersecurity requests information about current and future states of cybersecurity in the digital economy. As directed by Executive Order 13718, "Commission on Enhancing National Cybersecurity" (the "Executive Order"), 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 Secretary of Commerce was tasked by the Exective Order to direct the Director of the National Institute of Standards and Technology (NIST) 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.

Responses to this RFI – which will be posted at http://www.nist.gov/cybercommission – will inform the Commission as it develops its detailed recommendations.

DATES: Comments must be received by 5:00 PM Eastern time on [INSERT DATE 30 DAYS AFTER FEDERAL REGISTER PUBLICATION].

ADDRESSES: Written comments may be submitted by mail to Nakia Grayson, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899. Online submissions in electronic form may be sent to cybercommission@nist.gov in any of the following formats: HTML; ASCII; Word; RTF; or PDF. Please submit comments only and include your name, organization's name (if any), and cite "Input to the Commission on Enhancing National Cybersecurity" in all correspondence. Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials.

All comments received in response to this RFI will be posted at http://www.nist.gov/cybercommission without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information).

FOR FURTHER INFORMATION CONTACT: For questions about this RFI contact: Kevin Stine, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899, telephone (301) 975-4483, or cybercommission@nist.gov. Please direct media inquiries to NIST's Office of Public Affairs at (301) 975-2762.

SUPPLEMENTARY INFORMATION:

The digital economy has been a driver of innovation and productivity for several decades. The Internet is used every day by individuals, businesses, and government to make purchases, store sensitive data, and provide critical information services. These services and infrastructure have come under attack in recent years in the form of identity and intellectual property theft, deliberate and unintentional service disruption, and stolen data. Steps must be taken to enhance existing efforts to increase the protection and resilience of the digital ecosystem, while maintaining a cyber environment that encourages efficiency, innovation, and economic prosperity.

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, the President issued Executive Order 13718,[1] Commission on Enhancing National Cybersecurity, in February 2016.

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. According to the Executive Order, the Commission's recommendations should address actions that can be taken over the next decade to accomplish these goals.

The Secretary of Commerce was tasked by the Executive Order to direct the Director of NIST 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.

To accomplish its mission, the Commission shall, among other approaches, reference and, as appropriate, build on successful existing cybersecurity policies, public-private partnerships, and other initiatives; consult with cybersecurity, national security and law enforcement, privacy, management, technology, and digital economy experts in the public and private sectors; and seek input from those who have experienced significant cybersecurity incidents to understand lessons learned from these experiences, including

[1] Exec. Order No. 13718, Commission on Enhancing National Cybersecurity, 81 FR 7441 (February 9, 2016).

identifying any barriers to awareness, risk management, and investment. The Commission seeks broad input from individuals and organizations of all sizes and their representatives from sector and professional associations. The Commission also invites submissions from Federal agencies, state, local, territorial and tribal governments, standard-setting organizations, other members of industry, consumers, solution providers, and other stakeholders.

REQUEST FOR INFORMATION

The following questions cover the major areas about which the Commission seeks comment. They are not intended to limit the topics that may be addressed. Responses may include information related to or recommendations for other areas the Commission should consider.

Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials. Do not include in comments or otherwise submit proprietary or confidential information, as all comments received in response to this RFI will be made available publically at http://www.nist.gov/cybercommission. The Commission requests that each comment contain an Executive Summary, that is no more than one page in length, which identifies the topic addressed, the challenges, and the proposed solution, recommendation, and/or finding.

Based on the Executive Order and the Commission's initial deliberations, the Commission is seeking information on the following topics:

- Critical Infrastructure Cybersecurity
- Cybersecurity Insurance
- Cybersecurity Research and Development
- Cybersecurity Workforce
- Federal Governance
- Identity and Access Management
- International Markets
- Internet of Things
- Public Awareness and Education
- State and Local Government Cybersecurity

For each topic area, the Commission solicits information on current and future challenges, promising and innovative approaches to address those challenges, recommendations, and references to inform the work of the Commission. The Commission is specifically seeking input on the topic areas below:

Topic Area Challenges and Approaches

1. Current and future trends and challenges in the selected topic area;
2. Progress being made to address the challenges;
3. The most promising approaches to addressing the challenges;

4. What can or should be done now or within the next 1-2 years to better address the challenges;
5. What should be done over the next decade to better address the challenges; and
6. Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.

The Commission also seeks input on the following:

1. Emerging technology trends and innovations; the effect these technology trends and innovations will have on the digital economy; and the effect these technology trends and innovations will have on cybersecurity.
2. Economic and other incentives for enhancing cybersecurity.
3. Government-private sector coordination and cooperation on cybersecurity.
4. The role(s) of the government in enhancing cybersecurity for the private sector.
5. Performance measures for national-level cybersecurity policies; and related near-term and long-term goals.
6. Complexity of cybersecurity terminology and potential approaches to resolve, including common lexicons.

Kevin Kimball
NIST Chief of Staff
[FR Doc. 2016-18948 Filed: 8/9/2016 8:45 am; Publication Date: 8/10/2016]