**UNITED STATES DEPARTMENT OF COMMERCE**
**National Institute of Standards and Technology**
Gaithersburg, Maryland 20899

April 18, 2017

Dr. Kent Rochford
Acting Undersecretary of Commerce for Standards
and Technology
Director, National Institute of Standards
and Technology

The Honorable Mick Mulvaney
Director of the Office of
Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Dr. Rochford and Mr. Mulvaney,

I am writing you as the Chair of the Information Security and Privacy Advisory Board (ISPAB or "Board"). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-235) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, the E-Government Act of 2002, Title III, the Federal Information Management Act (FISMA) of 2002. The statutory objectives of the Board include identifying emerging managerial, technical, administrative, and physical safeguard issues relative to federal information security and privacy.

At our March 29-31, 2017 meeting, we heard presentations by employees of the Department of Homeland Security, the National Institute of Standards and Technology (NIST) and private sector participants about a range of security issues potentially impacting Federal information systems. The Board was briefed on several different vulnerabilities that that we believe the Administration should address as it develops its overall cybersecurity strategy. The Board offers the following observations for your attention:

- **Security of U.S. Government Websites.** The Board heard from the Information Technology and Innovation Foundation (ITIF) about a recent report ITIF published about security of Federal agency public facing websites. The ITIF found that several Federal government public facing websites have not implemented security measures already mandated for Federal agencies. It is the Board's view that, as part of the Administration's overall IT modernization strategy, agencies should take necessary steps to improve the security of these websites. Given the volume of public traffic to these sites, which are a primary means by which citizens engage with their government, their security against vulnerabilities and cyber attack directly impact public trust.

- **Federal Bug Bounty Programs.** The Board also was briefed on Federal bug bounty programs by the Department of Defense, referred to as "Hack the Pentagon", and by the Government Services Administration (GSA). Private companies use bug bounty programs to permit white hat hackers to report security vulnerabilities, in some cases for a financial reward and in others for recognition. While there can be extensive debate around the legality of third parties accessing government systems, and there are certainly limitations that would need to be placed on any government bug bounty program, the Board observed that the Federal government should develop an across-the-board strategy for developing bug bounty programs in government agencies. Given the significant

NIST

variation of cybersecurity capabilities of across agencies the Board recommends a coordinated whole-of-government, rather than agency-by-agency, approach to a bug bounty strategy. This should be based on the kind of cyber risk management principles envisioned in the President's cybersecurity executive order. Such a strategy should also inform development of more rigorous agency cybersecurity requirements built into acquisition contracts in order to reduce the number of software bugs acquired in the first place.

- **The Voting System as Critical Infrastructure.** The Board was briefed on the decision by DHS to designate the voting system as critical infrastructure and its intent DHS to establish an Election System Coordinating Council composed of state and local officials. While voting systems are predominantly within the jurisdiction and control of state governments, one factor that stood out to the Board was that Congress hasn't passed major legislation to aid states in modernizing the voting system since the Help America Vote Act was passed by the 107th Congress in 2001. That bill established a system of payments to states and created technical guidelines, among other issues, to promote the effective administration of Federal elections. While it is difficult for the Board to draw conclusions about the efficacy of cybersecurity of voting systems themselves, the Board believes that this topic should be studied further and that the Federal government may need to consider aiding states that deem it necessary to modernize their election systems. For example, legislation has been proposed in Congress that would enable states to apply for grants to help improve their overall cybersecurity posture. It may be possible to use such a program to allow state governments that, at their discretion, believe they need additional funds to modernize and secure their voting systems.

- **Distributed Denial of Service (DDoS).** Finally, the Board was briefed on the recent series of DDoS attacks and the Miria botnet involving infected Internet of Things (IoT) devices. It is evident that these types of attacks are likely to continue and, as with the security of U.S. government websites, the Board strongly encourages the Administration to ensure that agencies have strategies in place to ensure the continued viability of operations in the event of a potential attack.

These are just a few areas that may be worth further exploration to ensure the security of Federal IT systems and our voting infrastructure. The Board will continue to explore these and other security issues in the coming months and wanted to highlight a few of our observations from the meeting for consideration. We appreciate your consideration of these matters and look forward to continuing to work with the Administration going forward.

Christopher J. Boyer

Christopher Boyer
Chair
Information Security and Privacy Advisory Board