INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

ESTABLISHED BY THE COMPUTER SECURITY ACT OF 1987
[Amended by the Federal Information Security Management Act of 2002
And the Federal Information Security Modernization Act of 2014]

October 28, 2016

Dr. Willie E. May
Undersecretary of Commerce for Standards and Technology
Director, National Institute of Standards and Technology

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

Dear Dr. May and Mr. Donovan,

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.

Cybersecurity is a national and economic security issue for the nation. At our meeting October 27, 2016, we heard presentations by employees of both the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) regarding the President's Cybersecurity National Action Plan (CNAP) and plans for the transition to the incoming Administration. The letter offers the Board's view of several privacy and security issues that we believe should be priorities for the next Administration.

- **The NIST Framework for Improving Critical Infrastructure Cybersecurity ("Framework").** The Framework has proven to be a success and provides a valuable resource for both the public and private sectors. It serves as a model for how the public and private sectors can work together to raise the bar for cybersecurity. We strongly recommend that the next Administration continue to build upon the strong foundation provided by the Framework. The Board has also been briefed extensively on emerging threats related to the Internet of Things (IoT). Applying the Framework to the IoT and other emerging threat areas could also prove beneficial.

- **Role of NIST.** NIST is recognized as an expert level agency to address technical challenges related to cybersecurity by both the public and private sectors. The next Administration should continue to support NIST's collaborative leadership role, nationally and internationally, in addressing the many complex cybersecurity issues facing the nation.

- **Federal Information Technology (IT) Modernization**. There is a critical need to modernize the Federal IT infrastructure, a point that was recognized by the current Administration in the Cybersecurity National Action Plan (CNAP) signed by President Obama. CNAP proposed:

    - "An IT modernization fund to help "enable the retirement, replacement, and modernization of legacy IT that is difficult to secure and expensive to maintain" and,
    - "The formation of a new position – the Federal Chief Information Security Officer – to drive these changes across the Government."

In the Board's view, IT Modernization is a critical issue for improving the security and resiliency of Federal information systems. To help raise awareness to this issue, the Board has written several letters recommending and strongly urging migration away from legacy, outdated operating systems. We urge the incoming administration to make this a priority for security, resiliency, and privacy reasons. A consistent theme that agencies have raised with the Board is that the existing one-year budget planning and execution cycle makes it difficult to conduct long-term, forward looking planning. The next Administration should permit agencies greater authority and flexibility and support creation of this modernization fund to kick start the development and migration towards more resilient network architectures and technologies. We want to be perfectly clear: funding cybersecurity for legacy systems without modernizing federal IT is not cost-effective and far less likely to succeed. It is, therefore imperative that the next Administration work with Congress to ensure the initiative is fully funded.

- **Privacy and Civil Liberties Oversight Board (PCLOB)**. The Board has been briefed on multiple occasions by the PCLOB, which performs a valuable oversight role to ensure privacy in Intelligence Community related programs. The Board strongly encourages the next Administration to support the PCLOB and ensure it is provided adequate resources, including filling vacant PCLOB positions, to ensure that its vital work continues to protect Americans' privacy.

- **Centralized IT Infrastructure Services**. The current Administration proposed the establishment of a centralized service provider to manage IT for smaller agencies. The purpose is to encourage small agencies to outsource IT to a centralized entity within the Federal government versus managing IT in house. The Board supports this recommendation and believes that a centralized approach would help improve these agencies' security posture. It is well known in the cybersecurity community that there is a lack of cybersecurity experts, which is only exacerbated for smaller entities with limited budgets in both the public and private sectors. Enabling agencies to outsource IT and leverage the capabilities of larger, better-resourced entities could help improve the Federal Government's cybersecurity posture.

- **Clarifying Federal Roles and Responsibilities**. The Board has observed that, in many agencies, the Federal Chief Information Security Officer's (CISO) role is not empowered or can be at odds with other agency priorities. The CISO role should be elevated to a higher level of importance to ensure that cybersecurity is prioritized at a similar level as other mission critical functions. Further, the current Administration established a Federal CISO within the White House and, equally important, a Chief Privacy Officer within the Office of Management and Budget. The Board recommends that this model be expanded in scope to the department and agency level. The CIO-CISO relationship issue has been discussed for many years. We believe the time has come for the CISO to no longer be subordinate to the CIO so that CISOs may increase the visibility of security risks to senior management and ensure accountability for remediation of those risks.

- **Streamline Existing Programs and Enhance Utilization of Existing Cybersecurity and Related Tools and Resources**. The Board has observed that there are multiple, overlapping initiatives addressing similar issues across agencies. This leads to an inefficient use of resources both within the Federal government and among private sector partners who are called upon to support these programs. The White House and Federal CISO office should work with agencies to streamline and reduce overlapping initiatives and focus agencies' cybersecurity activities in their mission critical areas. There are also multiple tools that have been developed for agencies to better manage

cybersecurity risk, such as continuous diagnostics and software assurance tools that are available from both the Department of Homeland Security (DHS) and NIST. However, many of these tools are under-utilized. The next Administration should make it a priority for the Federal CISO to play an operational role working within agencies to promote and ultimately ensure the use of available tools. It is also imperative that agencies budgets are augmented to cover the out-year costs, to include licensing, personnel, hosting, and training, of new tools initially provided by agencies such as DHS.

- **Enhancing State and Local IT Infrastructure and Cyber Preparedness**. While DHS does offer various forms of cybersecurity assistance to state governments, inconsistent levels of state cyber preparedness remain because of insufficient budgetary, governance and human resource challenges. As state and local jurisdictions continue to embrace and invest in "smart cities" and other government service manifestations of the IoT, it is essential that OMB undertake an evaluation of states' budgetary needs for fundamental cybersecurity capacity building, their ability to convert DHS assistance to sustainable cybersecurity governance, and the extent to which grants and other federal cybersecurity programs result in measurable improvement in states' cybersecurity posture. Although state government information security policy and implementation oversight is *per se* outside the purview of this Board, our focus is on the effective application of federal cyber security policy and investment in which federal, state, and private sectors interoperate.

- **Internet of Things (IoT).** An area that is increasingly important is securing the Internet of Things. The Board was recently briefed on the series of distributed denial of service (DDoS) attacks that commandeered IoT devices to launch an attack on a domain name system service provider. It is clear more security controls must be built into IoT based products and services. The Department of Commerce, National Telecommunications and Information Administration, DHS, NIST and the Federal Trade Commission and other agencies are all exploring how to better secure IoT. Given the potential positive economic impact of IoT, but also acknowledging the cybersecurity risks, it is the Board's view that the US needs an overarching strategy for the IoT that provides protections while allowing the benefits of these new technologies to grow.

As we transition to the next Administration, the Board would like to thank the current Administration for its work and diligence toward improving Federal cybersecurity and privacy. There have been many success stories including most notably the NIST Cybersecurity Framework, the Cybersecurity Information Sharing Act of 2015, the Cybersecurity National Action Plan, Executive Order 13636, and the update to OMB Circular A-130. While commendable progress has been made, as with any complex issue such as cybersecurity, more work must be done. Since cybersecurity has emerged as a national issue, each Administration has seen it as a priority and built upon the good work of the prior Administration. We hope the next Administration uses this progress as building blocks to continue to improve our Federal cybersecurity posture. The Board would be happy to meet with you and the next Administration to further discuss these matters.

Sincerely,

Christopher Boyer
Chair
Information Security and Privacy Advisory Board