INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

November 20, 2014

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

Dear Mr. Donovan:

I am writing to 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 Security Management Act (FISMA) of 2002. The statutory objectives of the Board include identifying emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

At the Board's October 22-24, 2014 meeting, we received briefings on mobile device use within US Government agencies. Of particular importance was the difficulty of authenticating from these devices to access government systems. The initial requirement to deploy PIV Cards and their supporting infrastructure was initiated in 2004 by Homeland Security Presidential Directive-12 (HSPD-12), and NIST developed FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, envisioning the traditional desktop/laptop computing environment. This resulted in a system that assumed the existence of a physical card (like PIV) as a token, which is not appropriate for today's mobile computing

As a result, NIST is in the final process of publishing SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials (Draft)*, which introduces derived credentials. This leverages the investment of the Federal Common Access Card (CAC) deployment but extends the use of those credentials by linking them to credentials that are able to be stored in

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-2938 *** Fax: 301/975-4007

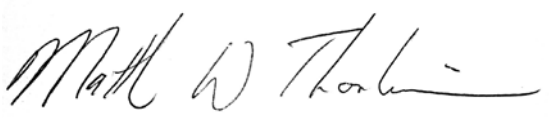
USB tokens, SIM cards, MicroUSB, TPM, and other logically separate, protected computing devices. Some agencies have noted their desire for an expeditious issuance of this document to provide official sanction to use such credentials.

However, the Board noted that first OMB memorandum M-06-16 would need to be amended, as it reads, "In addition to using the NIST checklist, I am recommending all departments and agencies take the following actions […] 2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access". The Board found that at the time, this and the other recommendations were sound; however, in light of the changing devices and the introduction of SP 800-157, the capability now exists to directly PIV-enable devices without the requirement for a physically separate factor.

Upon issuance of the final publication of SP 800-157, the Board urges review and reissuance of this OMB memorandum, in order to enable new remote work scenarios that are efficient, usable, and secure. Specifically, OMB should note that two-factor authentication is required for remote access, and that one factor can be provided by a device separate from the computer gaining access, *or* may be a leveraged derived credential stored in an embedded token as defined in SP 800-157.

The ISPAB supports our country's efforts to improve cybersecurity and looks forward to working with you.

Sincerely,



Matt Thomlinson
Chair
Information Security and Privacy Advisory Board

cc: Dr. Willie May
Acting Director of National Institute of Standards and Technology