INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

February 21, 2013

The Honorable Jeffrey Zients
Deputy Director for Management
US Office of Management and Budget
Washington, DC 20502

Dear Mr. Zients,

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-35) 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 February 13, 2013 meeting, we received a briefing on NIST's Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The ISPAB strongly supports the adoption of this publication for a number of reasons. First, NIST has regularly briefed ISPAB on its efforts for the past two years to update its security framework guidance, and this final revision has improvements that we think will increase security of federal information systems. The proposed changes in Revision 4 support the federal information security strategy of "Build It Right, Then Continuously Monitor," an approach that ISPAB supports. In addition, this framework has been amended to include privacy controls and implementation guidance based on the internationally recognized Fair Information Practice Principles in *Appendix J*. We believe this integration will bring much needed awareness and cooperation between privacy and security staff within agencies.

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

We also support Revision 4's new security controls and enhancements designed to address some of the newer challenges posed by advanced persistent threat (APT), supply chain, insider threat, application security, distributed systems, mobile and cloud computing, and developmental and operational assurance. Also helpful to agencies is its concepts of overlays and tailoring, allowing organizations to develop specialized security plans that reflect specific missions or business functions, environments of operation, and information technologies. Risk-based, specialized security plans are an essential aspect of realizing the intended outcomes from FISMA, rather than relying upon a paperwork-based reporting process for tracking FISMA compliance. We believe the security and privacy controls in this publication, along with the flexibility demonstrated in the implementation guidance, provide the necessary tools agencies need to implement effective, risk-based, information security programs.

Sincerely,

Matt Thomlinson
Chairman
Information Security and Privacy Advisory Board

cc: Patrick Gallagher, Director, NIST