INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

January 14, 2014

The Honorable Sylvia Mathews Burwell,
Director
Office of Management and Budget
Executive Office of the President
Washington, DC 20502

Dr. Patrick Gallagher
Under Secretary of Commerce for Standards and Technology
Director, National Institute of Standards and Technology

Dear Ms. Burwell and Dr. Gallagher:

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB). The ISPAB was originally enacted by the Computer Security Act of 1987 (P.L. 100-235) as the Computer System Security and Privacy Advisory Board. The charter was subsequently amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002, Section 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-4) and renamed it the ISPAB. 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 December 19-20, 2013 meeting, we received an update on the progress of NIST's development of its NIST Cybersecurity Framework, whose creation was required by the President's Executive Order (EO) on Improving Critical Infrastructure Cybersecurity. Cybersecurity is a critically important issue for American consumers, businesses, and the overall U.S. economy, and it presents a complex challenge. Creating the framework required a collective and collaborative effort among industry, academia, not-for-profits, standards organizations, and government organizations at various levels. The Board's agendas for the past several years have included numerous panels focused on how to encourage government and private-sector efforts to improve the status of cybersecurity in the U.S. In the Board's view NIST's Cybersecurity Framework provides an appropriate roadmap for that effort.

The Board would like to recognize NIST's hard work and collaboration in drafting the preliminary framework, including but not limited to, the five public workshops NIST conducted around the country. The Board observes that NIST went to great lengths to ensure transparency in the process and incorporate feedback from a wide range of stakeholders including academia, government, and the private sector. In particular, the Board would like to note key work done by a number of NIST personnel over the past year: Donna Dodson, Adam Sedgewick, Kevin Stine,

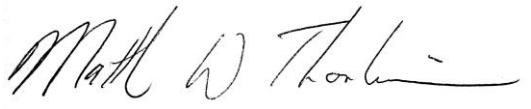
Matthew Scholl, Victoria Pillitteri, Ketan Mehta, Suzanne Lightman, Arnold Johnson, Kelley Dempsey, Lisa Carnahan, Jon Boyens, Judy Barnard, Murugiah Souppaya, Michael Bartock, Naomi Lefkovitz, and Angela Ellis.

While the Board discussed issues raised during the comment period around adoption, voluntary program incentives, and integration of privacy, we believe the current draft framework is a sound approach. We are optimistic that the framework release scheduled for February will fulfill the Executive Order's mission to provide a foundation for critical infrastructure cybersecurity.

One key issue the Board would like to stress is the importance of organizations ensuring privacy protections when implementing the cybersecurity practices described in the framework core. The Board recommends including a privacy methodology consistent with the Fair Information Practice Principles (FIPPs), and providing guidance on business processes to ensure privacy protections are in place as the framework is implemented. In our view, NIST could better accomplish this by having the description of the privacy protections more closely track the presentation of the framework core. The current draft privacy methodology in Appendix B both (1) outlines best practices for the protection of personally identifiable information, and (2) proposes business processes to ensure privacy is considered as the framework core is implemented. In our view, the portions of Appendix B discussing the protection of Personally Identifiable Information (PII) should be integrated into the data protection sections of the framework core, treating PII as a critical information asset similar to other sensitive information. The privacy methodology in Appendix B should focus on business processes or practices to ensure privacy is implemented as part of the core framework. Further, the privacy methodology should be embedded throughout the framework. We recommend that subsections be added to sections 1, 2, and 3 to expressly discuss the privacy practices outlined in the privacy methodology appendix.

We applaud the leadership of the White House, NIST, and DHS in driving improvements in national critical infrastructure cyber security through promulgation of Executive Order 13636 and the NIST Cyber Security Framework process. We look forward to working with you further on realizing the goals of the Executive Order.

Sincerely,



Matt Thomlinson
Chair
Information Security and Privacy Advisory Board