16-0000011-N

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 27, 2016

Dr. Willie E. May
Under Secretary 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 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 our meeting October 21, 2015 we had presentations by employees of National Institute of Standards and Technology (NIST) and National Security Agency (NSA) related to quantum computing. We discussed the critical concerns that would arise from the development of a cryptographically capable quantum computer, including making insecure all present and future uses of current public key cryptography. Even now communication sessions could be recorded, and then replayed and read when a quantum computer can break the key exchange that protected the communication.

Thus, there is a need for a quantum resistant key establishment algorithm well in advance of a quantum computer. By the time a capable quantum computer exists all existing public key cryptography will need replacement, including, for instance, certificate chains and code signing. There is no agreement on how to address this challenge. Without widely accepted standards and protocols there might be no interoperable commercial implementations, which would have negative impacts on privacy, security, and electronic commerce.

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

A plan for quantum resistance should provide a roadmap and timeline for getting to generally accepted standards, protocols, and, perhaps, competitions for necessary algorithms. Unfortunately not enough is known to lay out such a plan. The Board urges the creation of a strategy to develop such a plan. The strategy needs to describe what still needs to be learned and developed, and should consider how the new technologies are implemented, with the possibility that drop-in replacement are not the best, or even a viable, approach.

Public key cryptography was a new thing decades ago. When it was adopted it was writing on a clean slate, and the concept and its uses were all new. The same will not be true for quantum resistance technologies -- these will need to be adopted into an existing ecosystem, and on systems that often will need significant upgrades. While a relevant quantum computer may be years from fielding, replacing or upgrading systems will be a long and challenging endeavor, but one that is necessary to maintain the benefits public key cryptography has provided. For these reasons it is important to begin now.

The Board welcomes further discussion on this topic.

Sincerely,

Peter Weinberger, Ph.D.
Chair
Information Security and Privacy Advisory Board