UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-
OFFICE OF THE DIRECTOR

MAR 0 9 2016

Dr. Peter Weinberger
Chair
Information Security and Privacy Advisory Board
100 Bureau Drive
Gaithersburg, MD 20899

Dear Dr. Weinberger,

I wanted to personally express my thanks to you for the extraordinary leadership and commitment which you and the Information Security and Privacy Advisory Board (ISPAB or Board) have provided. The National Institute of Standards and Technology (NIST) and particularly Computer Security Division (CSD) fully recognize the importance of quantum resistant key establishment algorithm and necessity for having a well-laid out plan as suggested in your recommendation letter.

The CSD Cryptography group has been researching quantum resistant cryptography for over five years. In 2015, CSD decided to embark on a standardization plan for post quantum computing (PQC). The NIST PQC team recently released NIST Internal Report (NISTIR) 8015, "DRAFT Report on Post-Quantum Cryptography," for public comment on February 3, 2016. This IR shares NIST's current understanding about the status of quantum computing and post-quantum cryptography, and outlines NIST's initial plan to move forward.

Following the release of NISTIR 8015, the NIST PQC team introduced an initial post-quantum standardization plan at the Seventh International Conference on Post-Quantum Cryptography (PQCrypto 2016), February 24-26, in Fukuoka, Japan. The presentation of the plan described a call for proposals by the end of 2016 and a 5-7 year process for PQC standardization.

The CSD would welcome the opportunity to have the Board's assessment and feedback on PQC's plan based on the following aspects:

- Feasibility of the plan
- Engagement with research community and stakeholders
- General scope of PQC standardization
- Openness and transparency in selection of algorithms
- Collaboration with international and industry standard organizations

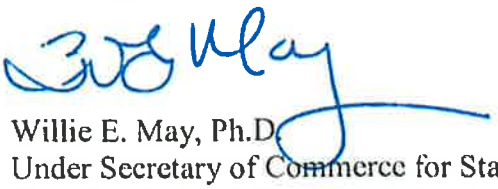
In addition, I would request that the Board track this work going forward to ensure the processes we define for developing cryptography in NISTIR 7977, "DRAFT NIST Cryptographic

Standards and Guidelines Development Process," are followed. The Board should periodically review our progress against quantum development timelines observed in the industries, research and also with federal agencies.

Finally, I would request that the Board conduct an assessment of the core cryptographic research capabilities of NIST, in particular, CSD. I'm interested in hearing the Board's opinion on whether NIST has made the necessary investments in human capital in order to execute on the PQC plan.

The work, recommendations and oversight provided by the ISPAB are important, valuable, and essential for NIST as an independent feedback mechanism on our work in Privacy and Cybersecurity. You have truly created a lasting impact on those who have participated in the NIST program at Gaithersburg.

Sincerely,



Willie E. May, Ph.D.
Under Secretary of Commerce for Standards and Technology &
Director, National Institute of Standards and Technology

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