Information Technology Industry Council

IT Alliance for Public Sector

April 22, 2014

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Via e-mail to: crypto-review@nist.gov

**RE: ITI and ITAPS comments on Draft NIST Interagency Report 7977, *NIST Cryptographic Standards and Guidelines Development Process***

The Information Technology Industry Council (ITI) and IT Alliance for Public Sector (ITAPS) appreciate the opportunity to comment on Draft NIST Interagency Report (NISTIR) 7977, *NIST Cryptographic Standards and Guidelines Development Process*.

ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's members comprise the world's leading ICT companies, with headquarters worldwide. ITAPS, a division of ITI, is an alliance of leading companies building and integrating innovative technologies for the government customer.

Our companies strongly support NIST's work developing computer security standards and guidelines for U.S. federal non-national security (NSS) information systems, as required under the U.S. Federal Information Security Management Act (FISMA) of 2002.[1] Many of our companies provide input into the development and selection of these standards and guidelines, including for cryptography. Our companies also are involved in an array of work in a multitude of global standards development organizations (SDOs) to develop cryptographic standards and guidelines for voluntary use in commercial and other markets. We are heavily involved in both of these work streams because cryptography is essential for security and privacy and is demanded by businesses, governments, and citizens worldwide.

Over the last decade, the use of cryptography has blossomed from a niche technology deployed mainly by governments and militaries/intelligence communities to becoming a ubiquitous, integral part of everyday life, as demonstrated by the widespread availability of commercial products supporting strong cryptography. In many ways, cryptography is now a core component of Internet and e-commerce development – and therefore economic growth. At the same time, ICT products and the cryptography they contain must be globally interoperable. The global nature of technology and cyberspace underscore the essential nature of strong, robust, and globally accepted and deployed cryptographic standards to enable interoperability, trust, and security.

[1] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf,

We appreciate NIST developing this NISTIR and soliciting public comment. Over the past nine months, the integrity of NIST's processes with regard to its development of cryptographic standards has been called into question since press reports surfaced in 2013 about the National Security Agency's (NSA) involvement in the development of the NIST SP 800-90A Dual Elliptic Curve Deterministic Random Bit Generation standard. We applaud NIST for putting this standard and related guidance back out for a 60-day public comment period in September 2013[2] as a testament to NIST's commitment to a transparent and trustworthy public process to rigorously vet its standards and guidelines. Full stakeholder input into the new review is just as important as it was during the original standard's development. It is imperative that trust in the integrity of the process be reaffirmed, both in terms of this particular standard and the NIST process overall. We hope and expect that this NISTIR will contribute to that reaffirmation.

Our comments below focus on two main areas: the content itself of NISTIR 7977, and NIST's processes developing and/or contributing to cryptographic standards development.

## NISTIR 7977 content: Suggested additions/clarifications

We are eager for this NISTIR to serve an important role in fully describing NIST's process in a way that highlights the processes' transparency (including ensuring that stakeholder input is sourced and traceable). The international community, in particular, needs to clearly understand what this process entails. We believe the NISTIR will benefit by the elaboration or addition of some key items.

**The NISTIR should clarify what NIST is and is not.** The NISTIR should clearly state that NIST is a technology-based, not policy-based, agency.

**The NISTIR should better describe the two very distinct roles NIST plays with regard to developing security standards.** The NISTIR begins by describing NIST's responsibility under FISMA for developing standards and guidelines for use in U.S. federal non-national security information systems. It is not until line 116, "Adoption of Existing Standards," that NIST's other role is described, i.e., that of being one of many stakeholders contributing technical expertise to voluntary, global, consensus-based standards developed by SDOs. These are two distinct roles that are important to differentiate, particularly for a global audience. Examples of how NIST works on cryptographic standards in each case would be illuminating. At the same time, NIST should make clear that the purpose of the NISTIR is to describe the former work, which is related to NIST's statutory role relative to U.S. federal information systems.

**The NISTIR should better explain NIST's work developing standards for U.S. federal information systems.** The NISTIR should make very clear that:

- This work is not specific to cryptography but, rather, is part of a much broader statutory requirement to develop computer security standards and guidelines;

[2] http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf

- Federal government standards developed by NIST are only applicable to federal non-NSS information systems;
- NIST standards and guidelines for federal information systems are developed using extensive stakeholder input;
- NIST standards and guidelines for federal information systems are found by many stakeholders to be highly secure and very relevant such that these stakeholders (including state and local governments, private entities, and even non-U.S. entities) voluntarily choose to implement them;
- There is a distinction between non-NSS and NSS systems and that NIST develops standards and guidelines for the former, and the NSA for the latter; and
- The requirement that NIST consult with the NSA on security standards development is only with regard to NIST's work developing standards for federal information systems under FISMA section 3543 Section 303 (b) (1), not with regard to NIST's other work contributing technical expertise to voluntary standards developed by SDOs.

**Suggestions regarding NIST process**

**NIST should more fully leverage open, global standard bodies for its U.S. federal-focused work.** While the U.S. Office of Management and Budget, via Circular A-119,[3] directs NIST to first consider the use of SDOs' voluntary consensus standards when the agency is developing standards for federal information systems, in many past cases, NIST has not found adequate standards in the cryptographic space, leading the agency to develop new standards for cryptography for U.S. federal information systems.

We strongly encourage NIST to devote more resources to contributing work to open, global SDOs that develop cryptographic standards used globally. NIST's cryptographic standards have a large impact commercially. As a result, where possible, NIST should adopt relevant international standards as the basis for Federal Information Processing Standards (FIPS).

By transitioning early work into the global work stream, NIST will achieve two positive outcomes. First, doing so will send a strong and much-needed message to global stakeholders about the U.S. government's commitment to a global, industry-led, voluntary, consensus-based, transparent, unbiased and trustworthy standards development process. Second, given the growing ubiquity of cryptography in both government and commercial markets, the work being conducted by global SDOs will increasingly be viewed as critical to driving trust in the Internet and e-commerce. Further, where NIST expects a broad range of industry to support its standards in their products, it will be increasingly important for that work to be progressed in open global SDOs.

[3] http://www.whitehouse.gov/omb/circulars_a119

We appreciate that this recommendation is not necessarily new or precedent-setting. In fact, NIST previously adopted two private sector-developed cryptographic standards for encrypting federal information in non-national security information systems. The Data Encryption Standard (DES), adopted by NIST as a federal standard in 1976, was based on work conducted by IBM during the early 1970s.[4] In 2001, NIST selected Rijndael, an algorithm submitted by two Dutch academics, to be the Advanced Encryption Standard (AES) for use by U.S. federal agencies.[5] We encourage the agency to refocus its efforts to participate in, and contribute technical expertise to, cryptographic work in SDOs to develop globally accepted, voluntary standards that can be used in the U.S. federal space.

## Conclusion

Thank you again for the opportunity to share our views on these important issues. We appreciate NIST's commitment to working with global stakeholders to develop cryptographic standards. We look forward to continuing to work with you.

Sincerely,

Danielle Kriz
Director, Global Cybersecurity Policy
Information Technology Industry Council

Pam Walker
Sr. Director, Homeland Security
IT Alliance for Public Sector
Information Technology Industry Council

[4] See http://www.nist.gov/director/planning/upload/report01-2.pdf. NIST retired DES as a federal standard in 2001.
[5] See http://csrc.nist.gov/archive/aes/round2/r2report.pdf and http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.