Summary of Public Comments on NISTIR 7977 (Second Draft, Jan. 2016)

Based on the draft January 2015 publication describing NIST's approaches and processes for its work on cryptographic standards and guidelines (*NIST Cryptographic Standards and Guidelines Development Process*, NISTIR 7977), multiple stakeholders provided comments and recommendations. Commenters included diverse members of the global cryptographic and standards development community. These comments were posted on NIST's website in March 2015.[1]

After considering all input, NIST will make a few changes in its approaches and processes, and is clarifying others. Those modifications are reflected in a revised version of the document, which is being posted on the NIST website.

This document summarizes by topic comments received from the public along with NIST's response to those comments. The *Note to Reviewers* accompanying the revised draft report also addresses many of these comments. All responses are incorporated into the final March 2016 version of the NISTIR.

1 NIST's Role in Cryptographic Standards and Voluntary Standards Developing Organizations (SDOs)

As with the first draft, a major focus of commenters was NIST's proper place in cryptographic standards development, both in terms of it's role in the community of standards developers, and in terms of what user communities should be NIST's first concern. One strong sentiment was that, notwithstanding NIST's statutory role in setting cryptographic standards for government agencies, NIST should consider the effects of its standards on industry as much the non-national security needs of agencies. A related assertion was that NIST standardization of NSA designed algorithms might be acceptable for Government use, but was unacceptable to industry, so should be strictly avoided.

A second related point, carried over from earlier comments, stressed stronger NIST participation in development and use of voluntary international standards wherever possible. This reflects industry wishing to implement different cryptography for different markets, either US vs. overseas, or Federal vs. commercial, and particularly a desire to avoid having to support many different national algorithms.

[1] Available at http://csrc.nist.gov/groups/ST/crypto-review/

NIST Response:
NIST will work with a diverse set of researchers, implementers and users to ensure its cryptographic standards and guidelines are secure, well-understood, robust, and trustworthy. NIST, as in the previous response, also acknowledges the importance of SDOs, particularly International SDOs, in this process, and will select voluntary consensus standards if its objectives can be achieved by doing so. NIST will pursue global acceptance for its cryptographic standards. To emphasize this point, NIST has added a new principle of "Global Acceptability" in the final version of NIST IR 7977. As it has in the past, NIST will work with SDOs to develop needed standards and will clearly indicate why it has adopted a particular approach. In working with SDOs or adopting their standards, NIST will consider the degree of active participation from researchers, industry and the user community.

The final version of NIST IR 7977 also reiterates NIST's commitment to submit its work to SDOs, with priority given to standards that fulfill a critical need, including those that result from competitions, and conformance-based standards.

2 Use of Formal Methods and Security Proofs

The second draft committed NIST to "pursue security proofs in the development of its cryptographic standards." While one group of commenters found this an improvement, they also sought an explanation of "what circumstances may make it impossible to include a security proof and what alternatives may be offered in its stead."

NIST Response:
Cryptographers gain confidence in the security of cryptographic schemes through cryptanalysis and security proofs. In cryptanalysis we study the internal structure of primitives or systems, or the mathematical problem on which its security is based, in an attempt to find the best attack on the primitive or system. Security proofs for cryptographic schemes typically show that breaking the scheme reduces to violating the primitive's assumed security properties or solving a problem thought to be mathematically hard. However, a security proof is not a guarantee of security. Proofs are usually conducted based on assumptions about the basic components of the scheme using a specific threat model; the correctness of the proof and the applicability of the threat model must be evaluated alongside the algorithm.

Both cryptanalysis and security proofs provide evidence for the security of a cryptosystem.

Cryptographers may not be able to prove that there is no efficient attack against a low-level cryptographic primitive. However, they may be able to

prove certain security claims regarding more complicated cryptographic schemes based on certain security assumptions on the underlying cryptographic primitives. There is also a tension between the strength of the security claim and the difficulty of finding a proof. While it may be relatively easy to prove certain security properties of a cryptographic scheme if a great deal is assumed regarding the strength of its underlying primitives, it is generally more difficult to develop similar proofs if relatively little is assumed.

In summary, security proofs are important tools for analyzing and vetting cryptographic algorithms being evaluated for inclusion in NIST standards and guidelines. NIST will look for, and evaluate, security proofs as part of its standardization process. However, security proofs are just one tool for analyzing algorithms. As described in NIST IR 7977, NIST will also look at available cryptanalysis that demonstrate an algorithm's vulnerability or resistance to new and old attacks in order to gain confidence that the security of an algorithm is well understood.

3 Undue Influence, Improper Influence, and FISMA consultation with NSA

The first draft drew comments on due process, undue influence and improper influence. This second draft included many revisions that attempted to clarify and improve NIST's process, and these revised sections drew considerably fewer comments. However, several commenters expressed concern over NIST's consultation with NSA, recognizing that the law requires it. One comment suggests that the NSA should best be thought of by NIST as equivalent to an intelligence agency of a foreign power, and concludes that the NISTR falls short of a process that ensuring NIST's integrity and independence. The commenter suggests annual reviews by: "the creation of additional outside paid review boards and conformance testing bodies," as well as publication of the minutes of NIST/NSA meetings.

Several commenters expressly urged NIST to expressly limit its consultations with NSA to the Information Assurance component of NSA and "to exclude any U.S. signals intelligences functions from the list of considerations to take into account when establishing standards."

Another commenter warns against "weighing the implications related to law enforcement and national security," and seems particularly concerned about NIST complicity in reviving something similar to "key escrow," warning that, "Weakening encryption algorithms for the benefit of law enforcement and national security is contrary to NIST's role in establishing and endorsing strong, robust, and secure standards." The commenter goes on to warn that, "the recent outbreak of a bug known as [Factoring RSA Export Keys (FREAK)] was caused by previous interference by the U.S. with cryptography."

NIST Response:
The second draft of NIST IR 7977 addressed the impact of law enforcement and national security concerns on NIST's cryptographic standards, stating "while being aware of implications related to law enforcement and national security, NIST focuses on its mission of developing strong cryptographic standards and guidelines for meeting U.S. federal agency and commerce needs." Upon review of the comments received on that draft, NIST determined this text did not accurately reflect NIST's process by suggesting that NIST regularly balances those equities against strong cryptographic standards.

The final version of NIST IR 7977 acknowledges the tension between NIST's mission to promulgate the use of strong cryptography, and the law enforcement and national security missions of other agencies. It clarifies that while NIST works closely with other agencies, it makes independent decisions, and remains committed to strong cryptography due to its vital role in protecting information and information systems. As part of this commitment, NIST will always develop standards and guidelines that promote the use of strong cryptography using open and transparent processes.

As part of NIST's process, NIST will continue to collaborate and consult with other federal agencies to identify, prioritize, and conduct work in cryptography. In particular, the Federal Information Security Modernization Act (FISMA) requires consultation with several agencies and Departments – OMB, the Departments of Defense, Homeland Security and Energy, the NSA, and the Government Accountability Office– in order to avoid unnecessary and costly duplication of effort, and to assure that NIST's standards and guidelines are complementary and compatible with those employed for the protection of national security systems and information contained in those systems.

NIST is also mindful of NSA's unparalleled cryptographic expertise, particularly in cryptanalysis. Several NSA designed algorithms adopted by NIST, including SHA-1, SHA-2 and DSA, have proved at least as good as their contemporaries and remain in use today. NIST will continue to consult with NSA on its cryptographic standards, but recognizes that it must have sufficient resources and capabilities to make independent decisions, and also that it must do so in a transparent manner. As such, the final version of NIST IR 7977 reiterates NIST's commitment to disclose comments from NSA, and provide attribution for contributions from the NSA and other participants in the standards development process.

4 Principles

NIST significantly revised its statement of principles in the second draft, adding usability as a principle. This section summarizes the comments received on those principles.

- **Usability:** The addition of a usability factor received favorable comments from several reviewers, one who noted that, "user errors are the primary cause or contribute to most security failures."

- ***Transparency***: One commenter stated that NIST should: "Publicly document the weights of evaluation factors in cryptographic competitions so as to allay doubts about the integrity of final selections."

  NIST Response:
  NIST has traditionally given broad general indications of the relative importance of selection factors in competitions. There are some concerns about committing to a specific, detailed weighting algorithm in advance:
  - Security is normally NIST's most important consideration, but has many facets, and can be very hard to measure with confidence or precision.
  - While performance can sometimes be measured with good accuracy, it also has many dimensions, and there are many platforms, each of different importance to different applications. Historically, NIST has looked for algorithms that have good performance overall, and not poor performance on any plausible platform.
  - Competitions focus much attention on a particular topic, and the community learns much during each competition. Committing to a detailed, rigid selection algorithm at the beginning of a competition might be fair and transparent, but may not give as good a selection as one that accommodates what is learned during the competition.

  A second commenter stated: "The transparency comments sound like a good start, but what does "in accordance with applicable law" mean here? The same question applies to l.78 and l.679. What would be a case in which a public comment could not be made public (l.51)? What laws rule other comments (l.54, l.78, l.679)? Depending on how broad this exception is the nice words about transparency are just lip service."

  NIST Response:
  A review of Federal law, regulation and policies about what information may, may not or must be released is beyond the scope of this summary. We note only that there are many laws, regulations

and policies intended to protect or control the release of information, including classified national security information, proprietary information, procurement sensitive information, and Personally Identifiable Information (PII). NIST is obligated by law to protect that information from disclosure.

The final version of NIST IR 7977 clarifies NIST's commitments to protect this information, and also describes how NIST will handle these cases. NIST will work with commenters to identify what information may be publicly disclosed. In the event that NIST receives restricted information that has or will materially affect a standard or guideline, NIST will make every effort to provide a meaningful summary of the comment. In all cases, NIST will publicly provide rationale for all substantive changes to documents.

That same commenter posed several specific about NIST's attribution of information received from NSA, attribution of collaboration with other agencies, specifically including NSA, if the NSA interactions include undercover NSA staff. But the commenter concludes: "In general it is more important to have the reasons and justifications for choices publicly available than to know exactly who came up with them — as long as the agency/institution to whom these individuals belong to is correctly named or this omission of attribution is stated appropriately. E.g. "Use A, it's secure, we've spent X hours on trying to break it" is received very differently depending on who says it. In any case this needs a statement of how this case would be handled."

NIST Response:
Yes, the reception of negative cryptanalysis (i.e., failed attempts to break an algorithm) depends on the analyst's reputation and expertise, and NIST will take that into consideration when adjudicating comments. However, positive cryptanalysis often can be demonstrated or verified.

The final version of NIST IR 7977 reiterates that NIST will track, post, and publicly respond to all comments received as a result of a request for comment on a draft FIPS or draft guideline, in compliance with applicable law. As part of this commitment, NIST will consider and acknowledge other agencies' comments, including comments from the NSA, whether they are provided during the formal public comment period or other stages of development.

- ***Openness***: The second public draft of NIST IR 7977 received suggestions to further open NIST's cryptographic standards process through the creation of either an additional outside paid review board or conformance testing bodies

and the establishment of positions for visiting cryptographers from around the world.

NIST Response:
The Federal Advisory Committee ACT (PL 463) governs the use of advisory committees and review boards. NIST's primary external advisory committee, the Visiting Committee on Advanced Technology, reviewed NIST's cryptographic standardization approach and its report can be found here. In addition NIST's Information Security and Privacy Advisory Board (ISPAB) meets quarterly throughout the year to monitor and advise on NIST's security activities, including cryptography, and reports its findings to the Office of Management and Budget, the Director of the National Security Agency and the appropriate committees of the Congress. Any additional review would have to fall under one of these venues.

The NIST Cryptographic Technology Group does take postdoctoral guest researchers from overseas, for example four overseas postdoctoral researchers participated as members of the SHA-3 selection team, and does occasionally host visiting academic cryptographers, as well as guest researchers from foreign government agencies. NIST, however, does believe it might be useful to establish a regular paid position for a visiting researcher and will explore the possibilities.

- ***Technical Merit***: Comments to the first draft stated that this term needed better definition and that NIST should do a better job of providing the information needed by others to judge technical merit. These concerns were apparently alleviated in the second draft since the only complaint that mentioned technical merit (discussed above) concerned weighing that with law enforcement and national security concerns.

- ***Balance***: Although the revised "Balance" principle in the second draft drew fewer comments than in the first draft, some commenters still desire stronger measures against any consideration of intelligence agency or law enforcement concerns.

NIST Response:
The second draft of NIST IR 7977 addressed the impact of law enforcement and national security concerns by stating "while being aware of implications related to law enforcement and national security, NIST focuses on its mission of developing strong cryptographic standards and guidelines for meeting U.S. federal agency and commerce needs." As noted above, NIST determined this text did not accurately reflect NIST's process by suggesting that NIST

regularly balances those equities against strong cryptographic standards, and removed this text from the "Balance" principle.

Within the *Federal Stakeholders* section, the final version of NIST IR 7977 acknowledges the tension between NIST's mission to promulgate the use of strong cryptography and the law enforcement and national security missions of other agencies. That section clarifies that while NIST works closely with other agencies, it makes independent decisions, and remains committed to strong cryptography due to its vital role in protecting information and information systems. NIST IR 7977 emphasizes that NIST will always develop standards and guidelines that promote the use of strong cryptography using open and transparent processes.

- ***Integrity***: One commenter noted that the statement that NIST will "never knowingly misrepresent or conceal security properties" was not sufficient to ensure integrity in the standards development process. That commenter suggested that NIST make a more proactive statement, such as "NIST will make every reasonable effort to ensure that military, intelligence and law enforcement agencies by their suggestions, review comments, or contributions do not compromise any security tool or algorithm recommended by NIST**."**

  NIST Response:
  NIST agrees with this comment, and has updated the "Integrity" principle to include a commitment to "make every effort to ensure that contributions to NIST's work from any organization do not compromise the security of any mechanism recommended by NIST."

- ***Continuous Improvement***: There were no comments on this principle.

- ***Innovation and Intellectual Property (IP)***: There were no comments on this principle.

- ***Global Acceptability:*** The final version of NIST IR 7977 includes the principle of "Global Acceptability" of cryptographic standards and guidelines. While this concept was described and valued within the second public draft, one commenter suggested that it should be elevated to a guiding principle.

  NIST Response:
  NIST agrees with this comment. The "Global Acceptability" principle states that "NIST recognizes the role of its cryptographic standards in assuring the competitiveness of U.S. industry in delivering these products and services, and is committed to ensuring that its standards and guidelines are accepted internationally."

5 Intellectual Property Rights

The first draft of NIST IR 7977 received several comments related to intellectual property rights. As of result of these comments, the second draft included a principle on "Innovation and Intellectual Property." This principle noted that while NIST will recognize and respect the value of intellectual property, it prefers to select unencumbered algorithms unless the technical benefits outweigh the potential costs of implementing patented technologies. NIST did not receive any comments on this new principle.

6 Pace of NIST Cryptographic Standards Development

The pace NIST cryptographic standards development drew comments in response to the first draft, and again in response to the second draft. Commenters expressed concern that the NIST process may not allow enough time for full review and consideration of proposed standards and guidelines. One commenter states: "NIST publishes security papers at a prodigious rate. So fast that reviews are deemed inadequate."

NIST Response:

NIST has a statutory requirement to develop strong cryptographic standards and guidelines to help federal agencies protect sensitive information on non-national security systems. To carry out that mission, NIST must be actively involved in advancing the fields of cryptography and cybersecurity to understand current capabilities and threats, and must also consult with agencies to prioritize its work based on their needs. While NIST needs to be agile to meet ever-changing needs, it also attempts to plan ahead for future needs as much as possible. The processes and procedures described in the final NIST IR 7977 are intended to allow NIST to meet those needs while also ensuring rigorous review of NIST's standards and guidelines, leveraging the internal capabilities within NIST and other federal agencies, as well as the extensive capabilities of the cryptographic research community.

7 Limited Number of Implementers

One commenter stated, "the best way to keep something secret is to have a very limited list of people on the standards and guidelines, around ten people." The comment went on to state that only five people should manage the implementation.

NIST Response:

NIST made no change. The strength of cryptographic protection does not, and cannot, rest in secret algorithms or methods, but rests only on the secrecy of keys. While small, highly-capable teams of experts may provide the best path for designing strong cryptographic algorithms, NIST believes

that proposed algorithms and standards should have the widest possible review to ensure they are secure and suitable for use.

8 Certified Executive Coach

One commenter suggested that NIST should add a Certified Executive Coach with a background in security to its organization.

NIST Response:

NIST made no change, but will consider this as part of future training and staffing needs.