Summary of Public Comments on NISTIR 7977 (Feb 2014 (First) Draft)

Based on the draft February 2014 National Institute of Standards and Technology (NIST) publication describing the principles 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 April 2014[1].

After considering all input, NIST is putting forward a variety of changes in its approaches and processes, and is clarifying others. Those modifications are reflected in a revised version of the document, which is being made available for further review to request additional stakeholder input.

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 January 2015 version of the NISTIR.

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

Many comments focus on NIST's proper place in cryptographic standards development, both as a contributor to and a user of the standards developed by the many U.S., regional, international and transnational SDOs that develop and issue standards that define, use, or incorporate cryptographic methods. This role is multifaceted, considering NIST's statutory responsibilities under the Federal Information Security Management Act (FISMA) as well as Executive Branch policy and directives. Most of these comments urge a stronger emphasis on working in and with SDOs. They advocate that NIST should favor using SDO cryptographic standards (particularly international standards) before developing new standards on its own. They also offer views about the importance of NIST's participation in SDOs' efforts and ensuring that NIST developed-standards be incorporated in voluntary standards, especially in international standards. One comment urged establishment of a new international process for cryptographic standards in the interest of curbing market fragmentation by many different national standards. The reasons stated for emphasis on SDOs included:

- Improve transparency

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

- Avoid undue influence
- Facilitate international trade by avoiding fragmentation
- Comport with OMB Circular A-119

NIST Response:
In the revised draft NISTIR, NIST clarifies its roles in the standards process as: 1) a developer of standards and guidelines under federal statute for use in U.S. federal non-national security information systems and as 2) a technical contributor/stakeholder in voluntary global standard development.

NIST also clarifies its policies on consideration of existing SDOs' standards and engagement with SDOs on new standards. This includes provisions to:

- Explicitly acknowledge the role and importance of SDOs, including international SDOs, in the development and acceptance of cryptographic standards.
- Pursue a global acceptance strategy for NIST's cryptographic standards, including aiming to prioritize resources to support this strategy.
- Select voluntary consensus standards if NIST's objectives can be achieved by doing so. When there is no community consensus and/or an existing standard, NIST will consider working with an SDO to develop a standard. If that is not a viable option, NIST will develop its own standard and give strong consideration to submitting this standard to an SDO.
- Indicate clearly why NIST has selected a particular approach.

NIST states that it will prioritize which NIST cryptographic standards and guidelines are brought to SDOs based on likely impact and need and industry interest. In addition, NIST clarifies the roles of NIST staff in working with SDOs, including stating the basis for determining NIST's participation.

The Institute makes it clear that when selecting priorities for working with SDOs or using their standards, a major consideration will be the degree of active participation from cryptography researchers, industry, and others in the user community.

2 Little Use of Formal Methods and Security Proofs

Several comments state that NIST makes little use of formal methods to specify cryptographic standards and it does not properly emphasize "security proofs" for cryptographic methods; they state that these shortcomings were not addressed in the draft. One comment calls the level of mathematical rigor in NIST standards "quite appalling," and asserts that: "Ultimately, nothing but formal methods can avert future disasters in cryptographic standards and their implementations in

code. Traditional forms of peer review of standards are simply inadequate for a task as important as the verification of major cryptographic standards."

NIST Response:
As part of its commitment to considering the technical merit of proposed standards and guidelines, NIST will pursue security proofs for proposed cryptographic algorithms or schemes. While not a prerequisite for consideration, security proofs are useful tools for analyzing and vetting cryptographic algorithms being evaluated for inclusion in NIST standards and guidelines. The 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. NIST will pursue these proofs, and encourage their development and analysis by the research community. In solicitations for proposed algorithms, NIST will ask for these proofs and, when available, include them in the public record when standards and guidelines are developed.

3 Due Process, Undue Influence and Improper Influence

The thrust of these comments is that the NIST standards development process should state stricter, more specific provisions for openness and transparency than are in the first draft. This, according to the comments, would constrain undue influence of powerful agencies (citing law enforcement and intelligence agencies) to subvert the security of NIST standards. It also would prevent NIST standards decisions being improperly influenced off-the-record. These comments seek a commitment by NIST to due process, meaning that NIST will always follows the stated process that provides openness and transparency, and any decision influenced by off-the-record inputs would be either unduly affected and/or improper. NIST is urged to explicitly state measures it will not engage in, including considering the "the signals intelligence needs of the NSA or any other intelligence or law enforcement need of any agency."

NIST Response:
NIST will never knowingly misrepresent or conceal security properties.

NIST now states that while being aware of implications related to law enforcement and national security, NIST will focus on its mission of developing strong cryptographic standards and guidelines for meeting U.S. federal agency non-national security and commerce needs.

NIST will disclose public comments received on drafts in accordance with applicable law. In all cases, NIST will make a best effort to disclose appropriate details. NIST also is creating more systematic and transparent record-keeping policies and procedures.

Stakeholders may submit comments regarding NIST's principles, processes and procedures — and NIST's use of them in developing cryptographic standards and guidelines. These comments should be directed to Chief, NIST Computer Security Division at crypto@nist.gov. All comments and NIST's responses will be posted on the CSD website.

4 FISMA and NSA

As noted above, a major point of many comments is that problems of bias and undue influence are best met by a process that ensures transparency and due process, ensuring that all parties get equal access and have due influence. FISMA requires consultation between NIST and NSA as well as other agencies before NIST issues information security standards and these consultations are not usually in the public record. Comments cite this as contributing to bias and undue influence in the standards process, particularly in the case of Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator), as noted below. In the view of some commenters, NSA should be treated at arm's length as any other party is and its inputs should be a part of the public record to ensure transparency and prevent undue influence; these comments state that the draft did not clearly address how this issue would be resolved.

NIST Response:

With NIST cryptographic standards and guidelines being used to protect national security systems under the Suite B program, the national security community, the NSA in particular, is an important stakeholder. NIST works closely with the NSA in developing cryptographic standards both because of that agency's vast expertise in cryptography and because NIST, under FISMA, is statutorily required to consult with the NSA and other agencies on standards. Although NSA has unparalleled expertise, NIST recognizes that it must have sufficient capabilities of its own to make independent decisions about recommendations and comments from the NSA.

NIST will disclose all comments on drafts, in accordance with applicable law. In all cases, NIST will make a best effort to disclose appropriate details. NIST also is creating more systematic and transparent record-keeping policies and procedures.

5 Dual_EC_DRBG

A strong thread running through several comments is that the draft fails to plainly acknowledge or explain NIST's failure to respond to the early Shumow-Ferguson warnings or several later warnings about the Dual_EC_DRBG included in NIST SP 800-90A. Moreover, they state that the draft does not adequately explain how the inherent conflicts that resulted in this failure would be prevented in the future by NIST's process.

NIST Response:
NIST erred in including the default elliptic curves points in its specification for Dual_EC_DRBG without an explanation of their provenance, particularly after researchers in the cryptographic community demonstrated how these points could conceal a backdoor in the algorithm. In the future, NIST will ensure that the provenance of any constants included in its standards and guidelines are fully described.

Immediately following news reports based on leaked, classified documents alleging that this algorithm contained not just a theoretical weakness, but an exploited backdoor, NIST solicited public comments on NIST SP 800-90A, and issued an ITL Security Bulletin[2] recommending that Dual_EC_DRBG no longer be used. Based on the public comments, and NIST's own review, Dual_EC_DRBG has been removed from later drafts of NIST SP 800-90A.

As part of an external review of NIST's cryptographic standards and guidelines program, NIST staff prepared a detailed presentation describing the development history of Dual_EC_DRBG and NIST SP 800-90A. This presentation, along with other background documents collected in response to Freedom of Information Act (FOIA) requests, are available on the NIST website[3]. Based in part on these materials, the review group developed recommendations for NIST on steps to strengthen its cryptographic standards and guidelines program. These recommendations, along with the public comments on the first draft of NISTIR 7977, led to significant changes to the processes and procedures that NIST will use to develop future standards and guidelines.

6 Principles

NIST received comments on the draft's statement of six principles that guide its cryptographic standards and guidelines efforts:

- ***Transparency***: Several comments suggest that transparency is aided by working more closely with voluntary SDOs, and urge a stronger commitment to that in the process. A second major transparency issue is the NIST-NSA relationship and interactions, and the degree of its visibility to the public.

  NIST Response:
  NIST now states clearly its commitment to working closely with voluntary SDOs. (See previous response under Heading 1, NIST's Role

[2] NIST Opens Draft Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, for Review and Comment.
http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf
[3] NIST Briefs Committee of Visitors. http://csrc.nist.gov/groups/ST/crypto-review/review_materials.html

in Cryptographic Standards and Voluntary Standards Developing Organizations, above).

NIST now states that while being aware of implications related to law enforcement and national security, it focuses on its mission of developing strong cryptographic standards for meeting U.S. federal agency and commerce needs. NIST stresses the importance of its access to sufficient in-house and other expertise to make independent decisions. In the interest of transparency, NIST will acknowledge all contributions to its standards and guidelines. To this end, NIST will make comments received on draft publications public, in accordance with applicable law. NIST will also properly acknowledge and name all persons who serve as a co-author on NIST publications, including co-authors at the NSA and other federal agencies.

- ***Openness***: One comment states that NIST should follow a "fully open process" when developing publications that are intended to be adopted by industry, emphasizing processes using an "open participation/competition model" or SDOs. NIST is also encouraged to commit to making all inputs to the standards process public. Other comments include suggestions about specific ways (e.g., social media) to make information available to the public.

  NIST Response:
  NIST will consider the use of open competitions to establish cryptographic standards particularly when no consensus exists yet around the best algorithmic approach. Competitions work best when a proposed algorithm or scheme requires a great deal of new cryptanalysis, as these competitions can focus the attention of cryptographers around the world. Decisions to use competitions will be made while recognizing and considering that these competitions are lengthy and resource intensive.

  NIST specifies that it will accept and make public all comments received on draft publications. In addition, NIST will provide rationale for all substantive changes to draft documents, either as a response to a public comment or in a separate description and justification for the change.

  NIST will make increasing use of social media to share information about its approaches, work, and proposals relating to cryptographic standards and guidelines.

- ***Technical Merit***: Comments state that this term needs better definition and that NIST should do a better job of providing the information needed by others to judge technical merit. Among concerns is that the only applicable criteria ("secure, efficient and promote interoperability,") appear under the principle of "Balance" in the draft.

NIST Response:
NIST focuses on its mission of developing strong cryptographic standards for meeting U.S. federal agency non-national security and commerce needs. NIST now states clearly that its priority must be on approaches that offer strong cryptographic protection to non-national security federal information systems.

NIST evaluations of technical merit will include a precise, formal statement of security claims, based on minimal security assumptions and supported as far as possible by documented cryptanalysis and security reduction proofs.

In addition, NIST will release available significant analyses and evaluations of algorithms or schemes included in NIST's cryptographic standards or guidelines, in accordance with applicable law.

- ***Balance***: One comment states that there is no mention of economics under this principle. Another says that balance is weighted in favor of enterprise stakeholders, and neglects individuals. A third opinion, appearing in two comments, is that the process should explicitly specify that intelligence and law enforcement agencies are never among the stakeholders to be weighed in the balance of NIST standards considerations.

  NIST Response:
  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 non-national security and commerce needs.

- ***Integrity***: Comments link this principle to preventing "undue influence" and see NIST's coordination with NSA as a major threat to NIST's integrity.

  NIST Response:
  Under FISMA, NIST is required to consult with several federal agencies – including the NSA– in order to avoid unnecessary and costly duplication of effort and to assure that NIST's standards and guidelines are complementary with those employed for the protection of national security systems and information contained in those systems.

  NIST clarifies the principle of integrity, noting that it follows agency-wide procedures to manage the risk presented by those conflicts, and ensures appropriate training for the staff working on these standards.

- ***Continuous Improvement***: The author of one comment is skeptical about NIST's commitment to date: "…actions speak louder than words. After NIST ignored serious objections to DES, ignored serious objections to DSA, and ignored serious objections to Dual EC, why should cryptographers believe that NIST is actually interested in feedback? If NIST's procedures have changed recently, why doesn't the draft say so?" Another comment urges the final NISTIR to discuss the response to vulnerabilities discovered after a standard is adopted and commit to addressing vulnerabilities publicly.

  NIST Response:
  The revised NISTIR states more clearly how NIST's procedures are being modified to provide more openness, transparency, and balance. It is committed to addressing vulnerabilities publicly and in a timely fashion.

- ***Usability***: One comment (representing a group of several companies) urges NIST to add a principle: usability. The concept of usability expressed may be related to notions of cryptographic robustness expressed in other comments.

  NIST Response:
  NIST is adding a principle to reflect the importance of "*usability*." This principle emphasizes that cryptographic standards and guidelines should be chosen to minimize the demands on users and implementations as well as the adverse consequences of human mistakes and equipment failures.

7 Cryptographic Module Validation Program (CMVP)

Several comments suggest NIST should specifically address Implementation Guidance (IG). One states that "often the implementation guidelines can impact development as much as a specific standard does." The NIST CMVP that tests conformance to NIST cryptographic standards is offered as an example. Similar rules should apply to the IGs, including an opportunity for public comment on new guidance, according to this comment. Moreover, the backlog and delay for CMVP testing is said to be "intolerable in a world where hardware development cycles are less than two years."

NIST Response:
NIST is taking steps to make the process of developing FIPS 140 Derived Test Requirements and Implementation Guidance more open, participatory, and transparent. As part of that process, these documents will be issued as NIST publications, and additions and modifications to these publications will undergo public review prior to finalization.

While there are many factors that impact the time necessary for a cryptographic module to go through the validation program, NIST will devote the resources necessary to avoid lengthy delays in the processes it is responsible for. NIST seeks to review test reports within 90 days of receipt, and is making changes to its resources, tools and processes to meet or exceed that goal.

8 Intellectual Property Rights (IPR)

IPR is a contentious issue in many standards of economic consequence, and similarly has been highly contentious in cryptographic standards. One comment joins IPR and concerns about possible subversion by agencies: "the threat of subversion by the agencies but also the problem of companies pushing modifications that give them IPR related benefits."

NIST Response:

NIST is adding a principle on "*innovation and intellectual property (IP)"* to emphasize that NIST seeks to incentivize innovation while protecting IP in the field of cryptography. Noting a strong preference among its stakeholders for solutions that are unencumbered by royalty bearing patented technologies, NIST prefers to select unencumbered cryptographic algorithms. NIST may also select encumbered algorithms (those with patent protections) if the technical benefits outweigh the negative implications.

9 Pace of NIST Cryptographic Standards Development

One comment criticizes the NIST process (largely, but not entirely focused on encryption modes of operation), saying: "in the past decade NIST has been rushing so many cryptographic standards out the door that the quality of review has obviously been compromised…. Why should these NIST publications be trusted? Who has actually reviewed the security of these cryptographic mechanisms, and how comprehensive was the review. NIST should delay standardization to wait for clear evidence of adequate public review, and should abort standardization if the public review does not produce a solid consensus on security."

NIST Response:

NIST is challenged to keep pace with cryptographic standards needs for a rapidly evolving, Internet driven world. Security is increasingly vital to the reliable functioning of information technology systems and all societal functions that rely on them. NIST recognizes the challenge and is stating more clearly the principles and processes necessary to ensure trust in its standards and guidelines—all of which depend upon the active participation of the cryptographic community.

NIST is investing greater resources in its computer security responsibilities and activities.

10 Old Standards, Risks and Economic Consequences

One comment argues that NIST standards often are much stronger than required by the actual threats facing most users. This comment states that most non-government and some government users don't need the high security mandated by NIST for government use, resulting in, "state-subsidized industry delivering expensive hammers to the federal government agencies that are often incompatible with that which the commercial sector adopts." An example cited is the NIST shift from 1024-bit RSA to 2048-bit RSA, since few users are likely to be attacked by an adversary powerful enough to factor a 1024-bit key, while non-cryptographic attacks like phishing are bigger real-life problems. A comment recommends adding an explicit mention that the federal government is the primary customer for NIST cryptographic standards and guidelines.

NIST Response:

Law and Presidential directives assign NIST with responsibility for developing strong cryptographic standards and guidelines for meeting U.S. federal agency non-national security and commerce needs. That mission is now stated clearly. NIST has no regulatory authority nor intent to require use of these standards and guidelines by other sectors or organizations. Those institutions make their own decisions about if or how to use NIST products.

NIST knows that its standards are often used to protect important information and may be attacked by powerful adversaries. In many circumstances there is little extra cost to cryptographic algorithms that resist cryptanalysis by the most powerful adversaries: ordinary commercial laptops, cellphones and tablets usually do run highly secure NIST algorithms efficiently. NIST does attempt to balance economic concerns (which primarily result from continuing to use very old equipment) with security. The cryptographic community has far more often criticized NIST for being too slow to retire older less secure methods, than for setting the bar too high.

Other commenters criticize NIST for being to slow to withdraw or at least "deprecate" older less secure standards, or for adopting methods that are less robust (easy to misuse or more difficult to use securely) than optimal. This is done, it is suggested, in the interest of better performance or because insufficient time was allowed for full study and analysis, or simply because NIST relied on NSA to vet an NSA- developed method.

NIST Response:

NIST now explicitly states that all cryptographic standards and guidelines must be maintained regularly in light of rapid technological advances, the specific applications and assets for which these standards and guidelines are used, the threat environment, and the tolerance for risk by a particular sector or organization. NIST is committed to periodic review and maintenance of all cryptographic standards and guidelines – including updating and possible

sunsetting. A newly produced overview of the life cycle process in the NISTIR describes how it will manage cryptographic standards and guidelines. That includes regular solicitation of public comment and feedback in line with NIST's principles of integrity, openness, transparency, and balance.