NIST Cryptographic Standards and Guidelines: A Report to the NIST Visiting Committee on Advanced Technology Regarding Recommendations to Improve NIST's Approach

FORWARD:

In July 2014, the National Institute of Standards and Technology (NIST) Visiting Committee on Advanced Technology (VCAT) submitted a report with findings and recommendations about NIST's approach to developing and managing cryptographic standards and guidelines[1].

The report is based on the work of a VCAT subcommittee along with recommendations from a distinguished panel of experts known as the Committee of Visitors (CoV). The COV was established specifically to review NIST cryptographic processes and provide their individual assessments.

NIST also received comments from public stakeholders based on a draft February 2014 publication describing NIST's approaches and processes for its work on cryptographic standards and guidelines (*NIST Cryptographic Standards and Guidelines Development Process*, NISTIR 7977) published for public review and comment.

After considering input from the VCAT and the public, NIST changed its approaches, engagements, investments and processes and is planning for additional changes to address the VCAT recommendations. Future plans involve clarifications and public statements on existing processes, updates to needed areas and introduction and training of new processes in the development of cryptographic standards and guidelines. These are specified in the revised version of NISTIR 7977, which is available for a second public review at the time of this report.

This report outlines NISTs response to many of the VCAT and COV findings and recommendations. It is organized largely to respond to categories of recommendations made by the VCAT

- [1] http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf

Openness and Transparency

- ***VCAT/COV**: It is of paramount importance that NIST's process for developing cryptographic standards is open and transparent and has the trust, confidence and support of the cryptographic community. That requires development of standards that are "best of breed" and untainted. NIST should develop and implement a plan to further increase the involvement of the cryptographic community in the standards development process. The agency should identify improvements to its processes and call out what those improvements are. NIST should establish a life cycle management procedure for all its standards and guidelines that supports its core principles; it should critically review all its standards and guidelines and evaluate whether to withdraw or revise them. This requires transparent decision processes on starting work in an area, choosing an approach to go forward, version management for all drafts from an early stage, detailed and individual dispositions for each and every comment received, a documentation of all design decisions, and procedures for regular revisions and emergency revisions. NIST should improve record-keeping and workflow management. It also should reflect whether participants have recourse to appeal decisions.*

  NIST Response: NIST clarified its principles and steps related to openness, transparency, balance, and integrity. Specifically, NIST now publically and clearly states that the Institute is focused on its mission of developing strong cryptographic standards for meeting U.S. federal agency non-national security and commerce needs while being aware of implications related to law enforcement and national security. NIST stresses the importance of its access to sufficient internal and other external expertise to make independent decisions.[2]

  NIST outlined a seven-step process for the life cycle management of its cryptographic standards process from identification of need, through regular review, potential updating, and sunsetting. The public's involvement and input is a milestone goal for each of these steps. When producing cryptographic standards or guidelines, NIST will provide a timeframe for reviewing and maintaining those documents – including possible updating and sunsetting. NIST will disclose all comments on drafts unless there is a clear legal prohibition, in which case NIST will make a best effort to disclose appropriate details as allowed. This involves formalizing policies and processes for handling informal and anonymous comments. NIST also is creating more systematic and transparent record-keeping policies and procedures.

  NIST issued a Federal Register Notice requesting comments on withdrawal of six FIPS. The standards proposed for withdrawal include FIPS 181-Automated Password Generator, FIPS 185-Escrowed Encryption Standard, FIPS 188-Standard Security Label for Information Transfer, FIPS 190-Guideline for the Use of Advanced

[2] http://csrc.nist.gov/groups/ST/crypto-review/index.html
http://www.nist.gov/director/cybersecuritystatement-091013.cfm

Authentication Technology Alternatives, FIPS 191-Guideline for the Analysis of Local Area Network Security, and FIPS 196-Entity Authentication using Public Key Cryptography.

NIST is instituting an appeals mechanism to provide greater assurance that NIST's cryptographic standards follow the stated processes. Appeals would be based strictly on assurances that the processes were followed, rather than the substantive content of the standard.

Changes to NIST's approaches are highlighted in the note to reviewers of the revised draft publication (NISTIR 7977) and are being publicized widely via NIST's website, press releases, and mailing lists and direct communications to stakeholders.

VCAT/COV: *NIST should clarify its roles as:*

1) *a developer of standards and guidelines under federal statue for use in U.S. federal non-national security information systems and,*
2) *a technical contributor/stakeholder in connection with voluntary global standard development.*

NIST Response: NIST clarified its roles in the standards process in the NIST IR 7977. NIST also states that the Institute will prioritize which NIST cryptographic standards and guidelines are brought to standards developing organizations, based on likely impact and need and industry interest. In addition, NIST clarified the roles of NIST staff in working with SDOs, including stating the basis for determining NIST's participation.

VCAT/COV: *NIST should address its objectives through voluntary consensus standards to the extent possible and explain the basis for a chosen path for standards development. NIST should verify whether processes in other organizations are compatible with its requirements for transparency and openness and open availability of standards and guidelines.*

NIST Response[3]: NIST clarified its role in working with Standards Developing Organizations (SDOs) and its policies regarding consideration of SDOs' standards and standards development capabilities. This includes provisions to:

- Explicitly acknowledge the role and importance of SDOs, including international SDOs, in the development and acceptance of cryptographic standards.

[3] NIST will continue to ensure its standards engagements are consistent and clear in the application of the US Standards Strategy: http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/NSSC/USSS_Third_edition/USSS%202010-sm.pdf

- 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. When selecting priorities for working with SDOs or using their standards, a major consideration for NIST will be the degree of active participation from cryptography researchers, industry, and others in the user community.

VCAT/COV: *Development of standards through open competitions should be encouraged where appropriate.*

NIST Response: NIST publically states in IR 7977 it intends to use open competitions to establish cryptographic standards where no consensus exists yet around the best algorithmic approach. This is done while recognizing and balancing that these competitions are lengthy and resource intensive.

VCAT/COV*: NIST should strengthen its efforts to make its cryptographic standards understandable and more easily usable by security engineers. Technical merit is first and foremost a question of security, but also incorporates considerations of efficiency, interoperability, and practical implementation.*

NIST Response: NIST added a principle to reflect the importance of "*usability*." This makes it clear that NIST cryptographic standards and guidelines are designed and selected to help minimize purposeful or unintentional misuse of cryptographic capabilities so that they: are easy to implement and difficult to circumvent; support workflow; and are readily incorporated into existing and future schemes and systems.

VCAT/COV*: NIST should ensure that cryptographic evaluations of new standards are conducted and released to the public.*

NIST Response: NIST states in IR 7977 that as a general policy, it will release available analyses and evaluations of algorithms or schemes included in NIST's cryptographic standards or guidelines, unless there are explicit legal considerations. Moreover, NIST will identify opportunities to include security proofs in cryptographic standards and guidelines, request proofs if they exist, and make them part of the public record when they are essential, practical, and available.

VCAT/COV*: The principle of integrity should be clarified to include a reference to the importance of avoiding – or appropriately managing – conflicts of interest.*

NIST Response: NIST clarified this principle, notes that it follows agency-wide procedures to manage the risk presented by those conflicts, and ensures appropriate training for computer security standards staff.

Independent Strength/Capability and Clarification of Relationship with NSA

VCAT/COV: *NIST should increase the number of technical staff with cryptographic expertise and explore expanding its programs to engage academia and outside experts. Among other things, this will allow NIST to continue to seek NSA's advice as it is evaluating decisions about cryptographic standards and guidelines by ensuring that it knows when to accept and when to reject that advice.*

NIST Response: Recognizing that NIST increasingly must support the research needed to advance the science and lay the foundation for future cryptographic standards – to the extent that resources permit – NIST has stated that the Institute intends to participate extensively in the community by:

- Continuing taking part in the work of SDOs.
- Continuing to submit papers on NIST research to public forums and presenting at and attending research conferences.
- Providing additional program committee members, speakers and reviewers for conferences and workshops.
- Increasing invitations to host guest researchers, postdoctoral fellows and visiting scholars.
- Increasing funding for both external (including academic) and internal research.

Notably, funding for NIST's work in cryptography-related programs has been expanded significantly with passage of the Fiscal Year 2015 federal budget. NIST directed an additional $6 million to its cryptographic computer security-related work. This increase will support internal as well as external efforts related to NIST's standards and guidelines.

Revised proposed procedures in the NIST document make it clear that it will disclose all comments on drafts unless there is a clear legal issue. This includes comments from NSA or any other government organization.

VCAT/COV: *NIST must be in a position to reject advice from NSA when warranted. The current requirement for interaction with NSA should be reviewed and changes requested where it hinders NIST's ability to independently develop the best cryptographic standards to serve the U.S. government and the broader community. NIST should restructure its relationship with NSA.*

NIST Response: NIST is committed to working more collaboratively and actively with the cryptographic community; recent budget appropriations will allow NIST to

bring more cryptographic experts on-staff and to support and take advantage of needed specialized expertise within the academic sector.

NIST is reviewing its current Memorandum of Understanding with NSA and will develop a revised version that will reflect current needs and the principles and processes stated in the newly published version of the draft NISTIR. This includes recognition that NIST focuses on its mission of developing strong cryptographic standards for meeting U.S. federal agency non-national security and commerce security needs. NIST also has stressed in the most recent draft NISTIR the importance of its access to sufficient in-house and other external expertise to make independent decisions.

Technical and Other Issues

VCAT/COV: *The VCAT notes that the members of the CoV made a number of very specific technical recommendations. The VCAT recommends that NIST work openly with the cryptographic community to determine how best to address such recommendations.*

VCAT/COV: *NIST should not try to fix the DUAL_EC algorithm in SP 800-90A but should instead reissue the standard with DUAL_EC removed.*

NIST Response: Immediately after public concerns over the security of Dual_EC_DRBG surface, NIST solicited public comments on NIST SP 800-90A, the publication that specified Dual_EC_DRBG. Based on the feedback received, and NIST's own analysis, NIST released a revised draft that removed Dual_EC_DRBG from the publication in April 2014. This revised draft also included several other changes to the document that were under development prior to the concerns over Dual_EC_DRBG. Certain unresolved issues related to the testing of cryptographic modules led NIST to release a second revised draft for public comment in November 2014. NIST will revise the draft accordingly, and expects to release the final publication in the first half of 2015.

VCAT/COV: *NIST should generate a new set of elliptic curves for use with ECDSA in FIPS 186. These should be generated by a public process such that the cryptographic community can be confident that the resulting curves were chosen pseudorandomly from among a set of high-quality curves. The set of high-quality curves should be described precisely in the standard, and should incorporate the latest knowledge about elliptic curves.*

NIST Response: Despite recent, legitimate questions over the provenance of the its recommended elliptic curves, NIST is not aware of any attacks on these curves when they are used as described in NIST standards and guidelines and implemented correctly. Still, over the fifteen years since these curves were published, advances in the understanding of elliptic curves within the cryptographic community have led to the development of new elliptic curves and algorithms whose designers claim offer better performance and are easier to implement in a secure manner. Some of these

curves are under consideration in voluntary, consensus-based Standards Developing Organizations, including the Internet Engineering Task Force and an associated effort with the Crypto Forum Research Group (CFRG), which NIST is participating in.

At the CRYPTO 2014 conference in August, 2014, NIST announced it was beginning an effort to reevaluate the current set of curves, and consider requirements and proposals for new curves. NIST's Computer Security Divison has drafted a formal solicitation for comments on FIPS 186-4, the standard that specifies the curves, which will be released in early 2015. The responses to this solicitation will assist NIST in determining what should be done with the existing set of curves, and identify the need for any new curves. In addition, NIST is planning a workshop to be held June 11-12, 2015 at its Gaithersburg campus to discuss elliptic curve cryptography standards. Meanwhile, NIST will continue to participate in the CRFG and IETF's process to evaluate new curves, and engage the cryptographic research community at conferences around the world.

***VCAT/COV**: NIST should evaluate whether there is sufficient reason to reopen the decision to recommend the KW and KWP cipher modes in SP 800-38F.*

NIST Response: NIST is not aware of any cryptanalysis on the key wrapping schemes specified in NIST SP 800-38F that would call the security of those schemes into question. Most recent criticisms of these schemes have focused on the lack of a security proof. However, NIST believes these modes have been well-analyzed by the community, and that the cryptanalysis conducted support the security claims made of these modes. One issue identified is a theoretical attack involving extremely long messages. While this is a highly impractical attack, particularly given the intended use case of the algorithm, the guideline has always included a mitigation for this attack- limiting the length of the messages that may be encrypted using this algorithm. These issues were known during the development of SP 800-38F and are discussed in Appendix A. Should new analysis or other observations raise new concerns over the security of these algorithms we will work quickly to evaluate them and take appropriate remediating action.

***VCAT/COV**: NIST should emphasize the adoption of cryptographic standards with provable security properties.*

NIST Response: Security proofs are useful tools for analyzing and vetting cryptographic algorithms being considered for inclusion in NIST standards and guidelines. In recent cryptographic standardization efforts, including our on-going work specifying block cipher modes of operation and the SHA-3 competition to select a new hash function standard, NIST asked designers to include any security proofs in submissions so that these proofs can be evaluated alongside the algorithm. NIST continues to ask for these proofs, when they exist, and include them in the public record when standards and guidelines are developed.

VCAT/COV: *NIST should ensure that cryptographic objectives are attainable in more than one standardized way, and at least one alternative is publicly available and royalty-free. NIST should, in exceptional cases, include patented solutions.*

> **NIST Response:** NIST has added a principle on "*innovation and intellectual property (IP)"* to emphasize that the Institute seeks to incentivize innovation while protecting IP in the field of cryptography. NIST commits to a strong, general preference for royalty-free cryptographic approaches whenever possible and practical. NIST also states that it may select encumbered algorithms (those with patent protections) if the technical benefits outweigh the negative implications. NIST will follow also follow the established concepts in the report on Use of Voluntary Standards in Support of Regulation in the US[4] and the US Final Rule on Standards Incorporated by Reference. [5]

[4] http://gsi.nist.gov/global/docs/Voluntary_Standards_USRegs.pdf
[5] http://www.gpo.gov/fdsys/pkg/FR-2014-11-07/pdf/2014-26445.pdf