KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS ON: DRAFT NIST INTERAGENCY REPORT 7977, CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS

18 April 2014

The Center for Democracy & Technology (CDT) is pleased submit these comments to the National Institute of Standards and Technology (NIST) on NIST Interagency Report 7977, "NIST Cryptographic Standards and Guidelines Development Process."[1]

NIST has long been recognized as a forum for unbiased technical research, analysis, and standards development. Cryptographic technologies are a critical technology component that supports assurance and trustworthiness in computing and networking environments. As such, these components are a particularly important aspect of the work of NIST's Computer Science Division.

Given the prominent role NIST cryptographic standards play in computing and networking contexts, it is crucial that NIST remain demonstrably free from bias or undue influence. NIST cryptographic standards are widely adopted, placing considerable pressure on NIST to be systematic, open, transparent, committed to well-defined principles and processes, and to be responsive to global concerns. We are pleased that NIST recognizes this and has initiated a review of its cryptographic standards, starting with NIST-IR 7977.[2]

Our comments begin with general comments on NIST-IR 7977. We then discuss the principles listed in the document as well as additional principles. Lastly, we consider mechanisms and outreach that we believe will further these principles.

I. General Comments

The document's title and abstract should make it clear that the document is a high level statement of the principles and procedures that NIST follows in the development of cryptologic standards and guidelines. A more descriptive title would be "The NIST Cryptographic Standards and Guidelines Development Process: Overview of Principles and Procedures."

---

[1] "NIST Cryptographic Standards and Guidelines Development Process," National Institute of Standards and Technology, NIST-IR 7977, (February 2014), *available at:* http://csrc.nist.gov/publications/drafts/nistir-7977/nistir_7977_draft.pdf.

[2] "Cryptographic Standards Development Process Review," National Institute of Standards and Technology, Computer Security Division, Cryptographic Technology Group, *available at:* http://csrc.nist.gov/groups/ST/crypto-review/index.html (accessed on 17 April 2014).

We were expecting to see much more detail on how NIST makes decisions when faced with competing proposals, configuration choices, and other trade-offs. While principles are by definition somewhat abstract, processes, procedures, and mechanisms should be well documented with clear rationales explaining how they each support the principles. The description in the appendix to NIST-IR 7977 of evaluation criteria for proposed block cipher modes is exactly the kind of evaluation specification we expected to see documented throughout the document, not just in the appendix. In order to adequately describe how NIST makes decisions, each genre of cryptographic primitive or cipher mode included in NIST Federal Information Processing Standards (FIPS) or Special Publications (SP) must have clear sets of evaluation criteria that support the overarching principles.

Finally, for each FIPS and SP we would like to see documented in those publications the efforts that NIST has engaged in to enfranchise the stakeholder community, from talks, to events, to smaller outreach efforts. To the extent that engagement is important for a sound standards process, that engagement should be documented in the standard.

II. Cryptographic Standardization Principles

The principles listed in NIST-IR 7977 are a great start, but we feel there are some missing – due process and avoiding undue influence — and that a few others – technical merit and integrity – could be refined.

A. Due Process

One principle that is not explicitly stated, but should be, is that of due process.[3] Due process requires fair treatment to all stakeholders throughout the standards process, ensuring there are adequate opportunities for stakeholders to object to or amend certain decisions and that no stakeholder or set of stakeholders are disadvantaged or privileged throughout the process. For example, NIST often works privately with the authors of a mode proposal or the winner of an algorithm design competition to further refine the proposal before committing it to a written FIPS or SP document. However, as this refinement occurs in private, there are other important interests that may be neglected, including those of the authors of competing proposals that may have had their proposals or designs rejected and may have technical objections or enhancements to these post-selection changes that should be heard before a draft goes out for public comment. Any changes to proposed algorithms or standard parameters should be fair and transparent, with check-ins with the larger community and clear, documented rationale for the changes grounded in technical merit. The recent case of SHA-3's post-competition standardization is an example of changes to algorithm parameters that proved problematic to a number of people in the cryptographic community.[4] NIST should examine past comments about the standards process and decide if there are certain operating procedures that could be adopted to reduce shortcomings of due process.

[3] The principle of due process should be stated on its own in this document as it only fits partially under a number of the principles already identified in the document, including integrity, balance, and transparency.

[4] Joseph Lorenzo Hall, "What the heck is going on with NIST's cryptographic standard, SHA-3?," Center for Democracy & Technology (September 24, 3012), *available at:* https://cdt.org/what-the-heck-is-going-on-with-nist%E2%80%99s-cryptographic-standard-sha-3/.

B. Avoiding Undue Influence

A key part of integrity is avoiding undue influence, which has the potential to undermine each of the other principles stated in this document. NIST should acknowledge that improper influence is a threat to NIST's interests and the public interest in developing secure, efficient, and interoperable cryptographic standards, and that vigilance in the standard-setting process from all participants – NIST staff included – is key to ensuring that all principles are upheld. To discourage undue influence, NIST should make all steps in the standard-setting process as transparent as possible, including documenting each feature of a cryptographic standard and the rationale behind choosing particularly critical parameters or features.

In addition, NIST should detail what mechanisms and process elements currently exist to mitigate sources of undue influence. For example, are NIST personnel trained to spot potential subversion? do they have mechanisms and procedures they can feel comfortable using to report potential instances of undue influence? NIST should go further than describing what mechanisms currently exist and affirmatively state as part of the principle of undue influence that NIST will not engage in weakening or biasing a standard – e.g., backdoors, trapdoors, or RNG state exposure – at the request of an intelligence agency or law enforcement entity.

C. Comments on Technical Merit

The principle of technical merit is not adequately defined. Certainly, the requirement that "security properties are well understood" – listed at the end of the paragraph on technical merit – contributes to technical merit, but there is certainly more to it. In this document, NIST must define what makes a particular standard or decision good. Are there evaluation criteria from past standards efforts that tend to result in a particularly good algorithm in practice? Vice versa, are there lessons about decision-making in standards setting processes that tend to weaken, impair, or undermine a standard?

Part of the definition of technical merit lies in the text associated with the balance principle, where the document stresses NIST's goal to "develop cryptographic standards that are secure, efficient, and promote interoperability." These three criteria, at a minimum, should be explicitly included and defined as part of the principle of technical merit. NIST must also describe how these three technical merit criteria interact: do they depend on each other? can any of them be absent? how are they evaluated during the standards process for different primitives, modes, and guidelines? are there other criteria that should be included in evaluating technical merit? Technical merit is the core consideration for the adoption of a cryptographic standard and providing a more detailed discussion of the components of technical merit is critical in this document.

D. Comments on Integrity

The document's explanation of the principle of integrity is overly narrow; integrity is much more than being impartial and objective. Integrity also involves sound construction, a lack of corruption, and honest conduct based on strong moral principles. NIST should describe a richer notion of integrity here and pledge in this document to conduct its standards activities with utmost integrity.

There are powerful adversaries engaged in the cryptographic standardization process. While we recognize that the intelligence community is an invaluable source of technical and theoretical expertise in cryptography, NIST must be more open and transparent about the extent of its collaboration with these agencies (both in formal and informal settings) and how these activities further the principles outlined in this document. NIST should also explicitly state measures it will not engage in. For example, it should be relatively easy for NIST to state in this document that never will a deliberate backdoor or intentional bias be introduced into a standard on behalf of the intelligence community or a law enforcement entity. Finally, NIST should outline administrative measures for NIST staff that are caught undermining standards processes, such as dismissal.

III. Mechanisms and Outreach

In addition to internal mechanisms mentioned above for NIST staff to report potential cases of undue influence, we also have comments on other possible mechanisms that could help improve NIST's standardization process. A critical question is: based on what evidence is a re-evaluation of a standard triggered? In the case of SP 800-90A – which contains Dual_EC_DRBG – the re-evaluation of that document appears to be based on significant "community commentary."[5] But certainly evidence of specific technical weakness should trigger a re-evaluation. Would internal evidence brought to light at NIST also trigger a re-evaluation and, if so, what kinds of circumstances might warrant a re-evaluation? While this set of triggers cannot be exhaustive or strict, they should be written down for illustrative purposes here.

There seems to be no type of lightweight publication between a press release and a Special Publication. NIST could better communicate with the public and the cryptographic community by posting more frequent public updates about cryptographic standards news and developments. For example, a blog-like venue on crsc.nist.gov for the cryptographic technology group could publish posts on current work, such as a series of posts that detail changes made to a winning competition algorithm during the post-competition standardization process. NIST could also use this opportunity to engage new audiences and encourage more people to get involved in security, cryptography, and cryptographic standardization activities and events.

In addition, NIST could expand the scope of some of its communication channels. For example, NIST could conduct outreach to non-cryptographic communities about the importance of cryptography for assurance. These broader outreach efforts should not just focus on cryptographers, engineers, and computer scientists, but also reach out to civil society, the cybersecurity community and policy audiences. These communities rely on cryptographic standards every day and NIST and the standards process itself could benefit from wider understanding of the value of cryptography and cryptographic standards. NIST could use an expanded but modest social media presence, with groups like Cryptographic Technology using those venues to keep interested stakeholders informed about current activities and events as well as engaging with the community directly.

Finally, NIST in its cryptographic standards role must engage with global interests explicitly, rather than implicitly. Since these standards are the building blocks of assurance online and in digital environments, NIST cannot afford to prioritize US interests or discount international

[5] "Supplemental ITL Bulletin For September 2013," National Institute of Standards and Technology, Information Technology Laboratory (September, 2013), *available at:* http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf.

perspectives. NIST should explicitly commit to recognizing international interests in its standards work.

IV. Conclusion

Thank you for the opportunity to comment on NIST-IR 7977. We offer our comments in the hope that the ongoing cryptographic standards review process will solidify NIST as an unbiased arbiter of technical cryptographic standards setting. These principles are a crucial first step in establishing a foundation for the detailed review work and process specification to come. The resultant post-review cryptographic standards process will be more robust for having engaged in this hard work.

For further information contact:

- Joseph Lorenzo Hall, Chief Technologist, (202-407-8825, joe@cdt.org)
- Runa A. Sandvik, Staff Technologist, (202-407-8838, runa@cdt.org)