2nd Round of Public Comments Received on NISTIR 7977: NIST Cryptographic Standards and Guidelines Development Process (Draft)

From: Jeffery [mailto:jeffery@dautya.com]
Sent: Friday, January 23, 2015 12:44 PM
To: crypto-review
Subject: cryptographic

RE: NIST Requests Round Two Comments on its Cryptographic Standards Process

Definition: Cryptographic, the science or study of the techniques of secret writing, especially code and cipher systems …

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 level below is the people that manage the implementation, around five people.

The people that actually implement are those that do because they can and are closely watched. This is hard because the watchers cannot know what they are doing. These people must design and build computer systems for Cryptographic use.

The disaster of computer system being hacked is a sign that too many people are involved in the three groups mentioned above.

The equal problem is that money is now in the hands of one percent of the world's population. This means that the wealthy have more money and power than the government to do what they want and that is to satisfy their overblown egos. My apologies for the very few who are sincere.

The 15 key people must be handpicked.

From: Beatriz Kelly Serrato [mailto:bebe@bebekellyserrato.com]
Sent: Friday, January 23, 2015 3:32 PM
To: inquiry
Subject: NIST IR7977: Round Two Comment on its Cryptographic Standards Process

Under the general comment there is one suggestion which might be considered. Since the technologies and the Cryptographic topography changes as well as the threat field and I might add this happens on a day to day basis.

An article to include an internal Certified Executive Coach who has a background in security might be a prudent and wise addition to the NIST organization. While your documentation might remain in tact addition internal coaching to the cyber culture and making this a requirement will keep your security environments on their toes. A Certified Cyber Security Coach would add so much to the NIST Security Culture. It is my professional opinion that this is a necessary and missing element in the security environment. A CCSC is not a consultant but an entity who knows what questions to ask the experts and security analysts of the environment before a breach or impending breach has happened.

Warmest Regards,
BeBe Kelly-Serrato
EC, FITSI

From: Eachus Lonny [mailto:lonny6@gmail.com]
Sent: Friday, January 23, 2015 4:46 PM
To: crypto-review
Subject: Cryptographic Standards Process

I am encouraged by the new Cryptographic Standards and Guidelines Development Process document (NIST IR 7977), in particular the section about openness and transparency.

Transparency and openness are essential to restoring public faith in NIST, much of which has been lost over the last 23 or so years. Among the primary reasons for the loss of faith in Government and NIST process was the Clipper Chip - Skipjack scheme, which not even in hindsight but at that time was widely considered to be -- not to put too fine a point on it -- bone-headed and irresponsible at best. Many considered it to be a transparent government power-grab. The fact that NIST attempted to move ahead with the program despite literally overwhelming public opposition and negative comments caused a progressive loss of faith in your organization, which has lasted more than two decades.

Recent revelations about likely weakened encryption using Dual_EC_DRBG had a similar effect. The result is plainly and simply that the public, including a possible majority of computing professionals, have little further trust in government in regard to cryptography.

I strongly suggest that at this point in time transparency and openness are not optional or suggestions but essential politically to the continued operation of NIST in this realm of endeavor.

Any proposed encryption standards must be provided to private-sector professionals AND the public for not just cursory but EXTENSIVE review before acceptance. There is no longer any real -- or even desirable -- alternative. Most professionals and the public do not have the resources of an NSA at their disposal, nevertheless history shows that subterfuge is eventually routed out. When it has inevitably been discovered our government's reputation as an honest representative of The People has suffered, and rightly so.

Let us not allow that to happen again.

Lonny Eachus
==========

From: Harris, Michael W. (CDC/OCOO/OCIO) [mailto:fnb0@cdc.gov]
Sent: Monday, March 16, 2015 9:09 AM
To: crypto-review
Cc: CDC OCOO-OCISO Data Call; Gatland-Lightner, Cheri (CDC/OCOO/OCIO); Flaherty, Colleen M. (CDC/OCOO/OCIO)
Subject: Comments on NISTIR 7977

CDC has no comments to provide on the *draft NIST Interagency Report (NISTIR) 7977, NIST Cryptographic Standards and Guidelines Development Process*.

Thank you for the opportunity to review and comment.

Michael Harris, CISSP
Information Technology Specialist (Information Security)
Office of the Chief Information Security Officer (OCISO)
Office of the Chief Information Officer (OCIO)
Office of the Chief Operating Officer (OCOO)
MWHarris@cdc.gov | 770-488-8052 office | 770-283-9589 cell

From: Gayn B. Winters, Ph.D. [mailto:gaynwinters@alum.mit.edu]
Sent: Tuesday, March 24, 2015 6:17 PM
To: crypto-review
Cc: crypto
Subject: NIST Interagency Report NISTIR 7977 "NIST Cryptographic Standards and Guidelines Development Process" January 2015 Draft.

To: crypto-review@nist.gov
Cc: crypto@nist.gov
Re: NIST Interagency Report NISTIR 7977 "NIST Cryptographic Standards and Guidelines Development Process" January 2015 Draft.
Date: March 24, 2015

The January 2015 Draft is a big improvement. In addition, the Summary of Public Comments on NISTIR 7977 (Feb 2014 (First) Draft) was quite helpful to compare how the current draft addresses comments on the first draft. The authors of both new documents are to be commended for their work.

General review comments:

A. Review comments on the first draft of NISTIR 7977 reflect a distrust of the NSA, and by extension of NIST processes. Suppose China sends NIST an email that says, "Hey, we've been studying elliptic curve E over field Z/p with base point Q. It has some neat properties, and China recommends that NIST adopt E for its elliptic curve encryption." Should NIST consider China's suggestion? A good test of the processes in NISTIR 7977, would be to answer "yes", even though we suspect that China knows a backdoor to encryption that uses E. Now, receiving such a suggestion from the NSA should be little different. Even though NIST is required to consult with the NSA, most independent security consultants, post-Snowden, would not trust a curve suggested by the NSA any more than one suggested by China. I certainly would not. Therefore we look for processes in NISTIR 7977 that politely look with great suspicion on suggestions for tools and algorithms from the NSA. NIST should get expertise and knowledge from the NSA, but should not blindly accept its tools and algorithms. NIST processes for analysis and acceptance of any suggestion, be it from the NSA, from China, or from any other source should be equally stringent. In particular, cryptographic technology should not be standardized without significant consensus from a wide swath of independent cryptographers. The current draft of NISTIR 7977 does not have an emphasis on public analysis and consensus for acceptance.

B. Of course, NIST could standardize, say an encryption method, even from a private and independent source, and the NSA, China's PLA Unit 1398, the UK's GCHQ, or other nation-state cryptography group could know how to crack this encryption method, remaining silent during and after the standardization process. One would hope that NIST, through its own efforts and its financial support of academic and other cryptography research would facilitate the discovery of the weakness and would quickly retire the standard. Such post-standardization life cycle efforts by NIST also need to be part of NISTIR 7977 [line 727].

C. Now if NIST were to publish a proof that a tool or algorithm received from China, the NSA, or another source in fact had no back doors and was totally secure then a consensus on standardization might well be easily achieved. After believing such a proof, I might recommend the proven technology to my clients, but I probably would wait until a huge number of non-government cryptographers also believed the proof and also were recommending this technology. NISTIR 7977 says roughly that NIST will "pursue" to find and use proofs [line 55]. I'd be happy if NIST worked with the NSA and other agencies on such proofs and would recommend such efforts be part of NISTIR 7977.

D. NIST publishes security papers at a prodigious rate. So fast that reviews are deemed inadequate. In light of post-Snowden caution around NIST processes, people naturally ask if these poorly reviewed papers can be trusted. It isn't going to help if NIST says, "It's ok, the NSA has reviewed it..." Look, not only does the current draft of NISTIR 7977 fail to convince that future NIST papers will receive good independent reviews, there was no indication that past NIST papers will retroactively receive good reviews. This is a very sad state of affairs, but it is fixable.

Some more specific review comments:

1. Clarity of the NIST Mission: To develop strong cryptographic standards and guidelines for meeting U.S. federal agency non-national security and commerce needs. This mission should be parsed: To develop strong cryptographic standards and guidelines for meeting 1. U.S. federal agency non-national security needs and 2. commerce needs. My point is that the needs of commerce should treated by NIST as equal to the needs of any federal agency. [line 202 ***Balance***]. For example, federal agencies may well be happy with NSA algorithms, but general commerce may not be.
2. I do not agree with the NIST Response (page 7 of Summary) to Technical Merit comments that NIST should give priority to non-national security federal information systems. NIST should always make commerce needs equally important. Such a priority statement doesn't seem to be in NISTIR 7977 explicitly, but there are several statements about NIST being legally required to give such a preference when so ordered by a government entity.
3. NIST's statement that it will "never knowingly misrepresent or conceal security properties" [Summary page 3; line 215 ***Integrity***] reminds me of Barry Bond's statement that he "never knowingly took growth steroids" when his hat/head size at the end of his career was three sizes larger than when he was a rookie. I would prefer 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." For NIST standards to regain the confidence of the security and general commerce communities, NIST processes should convincingly ensure by NIST public actions that its tools and algorithms do not compromise the privacy or the integrity of any commercial or private message being protected by NIST standards.
4. The FISMA requirement that NIST consult with certain federal agencies including the NSA to avoid duplication of effort and to maintain synergy of federal information protection efforts, but NIST can never in the future blindly accept a recommendation

from any public or private agency. What is important is that NIST actively regain and maintain its process integrity via the new NISTIR 7977. The current draft falls short.

5. NIST should consider resolving the conundrum of needing NIST output frequently and needing adequate public reviews of such output by the creation of additional outside paid review boards and conformance testing bodies. Such a review board should be established to review annually the entire Cryptographic Technology Group. [lines 316 and 326]
6. Minutes of the monthly NIST/NSA meetings should be published. [line 377]
7. Independent review boards should have the power to reject a proposed standard, say if NIST could not convince the board that the NSA or another agency has not compromised the standard. [page 4; lines 47, 403, and 464]
8. The NISTIR 7977 Development Process itself should undergo regular review and updates at, say, an annual frequency.

Requested Comments [line 125]:

NIST Question	**Comment**
Do the expanded and revised principles state appropriate drivers and conditions for NIST's efforts related to cryptographic standards and guidelines?	Yes, but if the word "appropriate" were replaced by "adequate" then No. Neither the integrity of NIST processes in face of NSA influence, nor the issue of adequate review are satisfactorily answered. [A, C, D]
Do the revised processes for engaging the cryptographic community provide the necessary inclusivity, transparency and balance to develop strong, trustworthy standards? Are they worded clearly and appropriately? Are there other processes that NIST should consider?	No. "Trustworthy" standards need public confidence that the NSA or another agency have not added or know of backdoors or other weaknesses to their contributions. Wording isn't an issue. Different new processes are necessary to separate NIST from NSA and other related agency influence. After-standardization research efforts should be funded as part of all life cycles [B].
Do these processes include appropriate mechanisms to ensure that proposed standards and guidelines are reviewed thoroughly and that the views of interested parties are provided to and considered by NIST? Are there other mechanisms NIST should consider?	No. Cf. A, C, 2, 3, 4, and 7 above. Regarding 7, if NIST won't vest veto power to independent reviewers, such experts will tend to not participate. Lack of review resources also seems to be a problem. Cf. 5 above.
Are there other channels or mechanisms that	Yes. More paid outside reviewers including an

NIST Question	Comment
NIST should consider in order to communicate most effectively with its stakeholders?	annual review of the Cryptographic Technology Group. Cf. D and 5 above.

Respectfully submitted,
Gayn B. Winters, Ph.D.

--
Gayn B. Winters, Ph.D.
Technology Consultant
Profile: www.linkedin.com/in/gaynwinters
Blog: http://gaynwinters.wordpress.com
Email: gaynwinters@alum.mit.edu

From: Steve Lipner [mailto:slipner@microsoft.com]
Sent: Thursday, March 26, 2015 2:06 PM
To: crypto-review
Cc: Brian LaMacchia
Subject: Comments on revised draft Cryptographic Standards and Guidelines Development Process

Microsoft Corporation is pleased to submit comments on the second draft of NISTIR 7977, Cryptographic Standards and Guidelines Development Process. We have provided overall comments in letter form as well as specific suggested modifications to the draft.

If you have any questions about these comments, please feel free to contact Brian LaMacchia (bal@microsoft.com) or me.

Thank you for the opportunity to comment on this important document.

Sincerely,

Steven B. Lipner
Partner Director of Software Security
Trustworthy Computing Security
Microsoft Corporation

25 March 2015
National Institute of Standards and Technology
Information Technology Laboratory
Crypto-review@nist.gov

Subject: Comments on revised draft Cryptographic Standards and Guidelines Development Process (NISTIR 7977)

Microsoft Corporation appreciates the opportunity to submit comments on the subject draft. Overall, we believe that the draft is a strong document and one that will go a long way toward ensuring the credibility of NIST cryptographic standards and guidelines. In particular, we believe that the articulation of specific principles that guide NIST's work in cryptography will help stakeholders understand and trust the steps that NIST takes. In particular, we believe the commitment to transparency, openness, technical merit, and integrity will resonate with the community.

We also consider the discussion of public notice and review to be valuable. In particular, the commitment to track, post, and respond to all comments received in response to a draft will go a long way toward addressing some of the concerns that have been raised in the recent past. We also found the description of policies and processes for management of standards and guidelines to be helpful both as an explanation of what stakeholders should expect and as a set of commitments that stakeholders can rely on.

We do have a series of suggestions for modifications that would strengthen the document. Several of these suggestions have to do with the global acceptability of standards and guidelines. We believe that global acceptability rises to the level of a principle that should guide NIST's processes at a fundamental

level. While we are well aware that NIST develops cryptographic standards and guidelines in response to a statutory requirement related to the protection of unclassified but sensitive information, NIST is also a part of the Department of Commerce and has a significant role in contributing to the competitiveness of U.S. industry. NIST cryptographic standards and guidelines are the foundation of many information technology products and services that are developed by U.S. suppliers and sold globally. We believe that NIST should recognize the role of its cryptographic standards in assuring the competitiveness of U.S. industry as fundamental.

We have suggested several modifications to the draft with the aim of strengthening the global acceptability of NIST cryptographic standards and guidelines. In addition to identifying global acceptability as a principle for NIST's cryptographic standards and guidelines development process, we have suggested that NIST:

- Commit to establishing positions for visiting cryptographers from around the world who would participate in and help shape NIST's research, standards and guidelines in cryptography.
- Commit to a preference for working with and through international standards development organizations (SDOs) to develop cryptographic standards and guidelines that do not rise to the level where a competition is required and to adopt cryptographic standards and guidelines that NIST finds it necessary to develop independently.
- Publicly document the weights of evaluation factors in cryptographic competitions so as to allay doubts about the integrity of final selections.
- Commit to a preference for submitting the results of cryptographic competitions to SDOs.

We believe that adoption of the suggested modifications will help to strengthen the document and to ensure that the reputation and credibility of NIST's cryptographic standards and guidelines remains strong.

Thank you again for the opportunity to submit these comments. We would be happy to discuss these recommended modifications, or any other aspect of the draft with you.

Sincerely,

Steven B. Lipner
Partner Director of Software Security
Trustworthy Computing Security

From: Amie Stepanovich [mailto:amie@accessnow.org]
Sent: Friday, March 27, 2015 10:01 PM
To: crypto-review
Cc: Drew Mitnick; Jack Bussell
Subject: Comment Submission: NIST IR 7977 (Second Draft)

To Whom It May Concern -

Thank you for the opportunity to provide feedback on the Second Draft of NIST IR 7977. Please find attached comments from Access.

If you have any questions or comments, you can contact me at amie@accessnow.org. Please confirm receipt of this email and the attachment.

Thank you,

Amie Stepanovich

--
Amie Stepanovich
Senior Policy Counsel
Access Washington, D.C. | accessnow.org

tel: +1.888.414.0100 ext. 702
@astepanovich
PGP: 1C1DA0C7
Fingerprint: CBBE 4CF3 84B5 FCA7 3BAA F3D0 FF72 6BC2 1C1D A0C7

In the Matter of NIST Cryptographic and Guidelines Development Process NIST IR 7977 (Second Draft)

March 27, 2015
Submitted via email to crypto-review@nist.gov

We write today to comment on the second draft of the Cryptographic Standards and Guidelines Development Process, published earlier this year by the National Institute for Standards and Technology ("NIST"). Specifically, we commend NIST on the improvements made in this updated draft, while noting some new and outstanding issues. We ask again that NIST explicitly circumscribes its relationship with the Signals Intelligence mission of the NSA and the Intelligence Community.

First released in February of 2014, the NIST Cryptographic Standards and Guidelines Development Process ("IR 7977") "outlines the principles, processes, and procedures of NIST's cryptographic standards efforts."[1] The goal was to help ensure that any adopted standards are "robust and have the confidence of the cryptographic community." This is especially important as the standards developed by NIST are widely used as the basis for secure communications across the internet.[2]

After a period of public comment, to which Access and a coalition of other organizations and companies responded,[3] the second draft was published January 23, 2015.[4] Access applauds NIST for the new draft — which expands upon and strengthens the language behind important principles first set out in the previous draft — and for actively and transparently engaging with the public on these important issues. Our further comments follow.

Introduction of Usability principle

The original draft of IR 7977 outlined six principles that NIST would adhere to when evaluating proposed cryptographic standards: Transparency, Openness, Technical Merit, Balance, Integrity, and Continuous Improvement. In our previous comment we had requested the addition of a seventh principle: Usability. Specifically, we said, "[c]ertain implementation

[1] National Institute of Standards and Technology, NIST Cryptographic Standards and Guidelines Development Process (First Public Draft), *available at* http://csrc.nist.gov/publications/drafts/nistir-7977/nistir_7977_draft.pdf.
[2] *See* Matthew Green, *On the NSA*, A Few Thoughts on Cryptographic Engineering (Sept. 15, 2013), http://blog.cryptographyengineering.com/2013/09/on-nsa.html.
[3] Letter from Access, et al., to NIST, April 19, 2014, *available at* https://s3.amazonaws.com/access.3cdn.net/73934b6b48cbc48268_oim6bx0jn.pdf.
[4] National Institute of Standards and Technology, NIST Cryptographic Standards and Guidelines Development Process (Second Draft) (2015), *available at* http://csrc.nist.gov/publications/drafts/nistir-7977/nistir_7977_second_draft.pdf.

errors may be anticipated or planned for such that it would render the implementation of a standard unsafe."[5]

In the updated draft, NIST added two additional principles, including one for Usability.[6] NIST notes that adherence to a principle of Usability will, "minimize the demands on users and implementer as well as the adverse consequences of human mistakes and equipment failures." This is an important addition in ensuring secure communications by all users, since "[e]ven theoretically strong cryptography standards may be exploited in practice."[7] User errors are the primary cause or contribute to most security failures.[8] By acknowledging this reality and introducing this principles, NIST has helped ensure stronger security protections designed for the real world.

Commitment to providing mathematical proofs

The second draft of IR 7977 is also much-improved by the inclusion of language outlining NIST's commitment to providing security proofs. Under the principles of Transparency and Openness (which were merged from the prior version), NIST has stated that "[a]s a general policy, [it] will release any significant analyses and evaluations of algorithms and schemes." It also committed to pursue security proofs, as often as possible, during the development of its standards and to encourage the participation by the research community. These positive steps help create more secure standards as public participation helps discover flaws and vulnerabilities that would otherwise go unnoticed. However, more guidance should be provided on what circumstances may make it impossible to include a security proof and what alternatives may be offered in its stead.

NIST's relationship with the NSA

As we have previously explained, the development of IR 7977 was the product of questions about the relationship between NIST and the U.S. National Security Agency ("NSA"). Specifically, NIST is legally required to consult with NSA on the establishment of cryptographic standards, a relationship that the NSA has previously abused on at least one occasion by intentionally weakening cryptographic standards, undermining the public's trust in NIST.[9]

---

[5] Letter from Access, *supra*, note 3.
[6] The second new principle is one of Innovation and Intellectual Property. This principle states that it is preferable that new standards are unencumbered by intellectual property restrictions.
[7] Letter from Access, *supra*, note 3.
[8] *See* Alma Whitten & J.D. Tyger, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*, In Security and Usability: Designing Secure Systems That People Can Use (eds. L. Cranor & G. Simson, O'Reilly, 2005) pp. 679-702; *see also* Mike Hearn, Usability of Crypto Software, Medium (Mar. 5, 2014), https://medium.com/bitcoin-security-functionality/d04ea6a2c771.
[9] James Ball, Julian Borger & Glenn Greenwald, *Revealed: How U.S. and U.K. Spy Agencies Defeat Internet Privacy and Secuirty*, The Guardian, Sept. 5, 2013, *available at* http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

The NSA's dual missions of both Information Assurance (protection of systems, the mission under which NIST coordinates with NSA) and Signals Intelligence (electronic surveillance) has been criticized by both civil society as well as the President's Review Group on Intelligence and Communications Technologies.[10] The dual mandate leads to one mission, typically Information Assurance, being steamrolled by the other. To its credit, NIST has added several key provisions to limit the ability of the NSA to unduly influence its standards setting mission. While we commend the addition of language to IR 7977 on NIST's commitment to guarding against undue or improper influence, we reassert the need for NIST to expressly limit consultation with the NSA to its Information Assurance mission, and to exclude any U.S. signals intelligences functions from the list of considerations to take into account when establishing standards.

Competing Considerations

Under the Balance principle, NIST now expressly reserves the right to weigh "implications related to law enforcement and national security" against other criteria. NIST also includes security concerns when evaluating the Technical Merits of a proposed standard. We strongly urge NIST to remove these considerations from the standards development process.

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. Weak cryptography makes users vulnerable to an array of bad actors.[11] For the past two decades, cryptographers have loudly concurred that any back doors or vulnerabilities, even for the sole use of legitimate government investigations, will have harmful effects on all users.[12] In fact, the recent outbreak of a bug known as "Freak" was caused by previous interference by the U.S. with cryptography.[13] That bug caused vulnerabilities in over five million websites, including news organizations, retail stores, and financial institutions.[14]

---

[10] Liberty and Security in a Changing World, President's Review Group on Intelligence and Communications Technology (2014), p.189, *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
[11] *See generally* Bruce Schneier, Web Snooping is a Dangerous Move, CNN iReport, http://edition.cnn.com/2010/OPINION/09/29/schneier.web.surveillance/index.html (Sept.29, 2010).
[12] *See, e.g.,* Nadia Heninger and J. Alex Halderman, Tales from the Crypto Community, Foreign Affairs (Oct. 23, 2013), *available at* http://www.foreignaffairs.com/articles/140214/nadia-heninger-and-j-alex-halderman/tales-from-the-crypto-community; Jeffrey Vagle, Cybersecurity and the Risks of Law Enforcement Backdoors, REGBlog, http://www.regblog.org/2014/12/22/vagle-cybersecurity-and-back-doors/ (Dec. 22, 2014).
[13] Craig Timberg, 'FREAK' Flaw Undermines SEcurity for Apple and Google Users, Researchers Discover, Washington Post (March 3, 2015) *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/03/freak-flaw-undermines-security-for-apple-and-google-users-researchers-discover/.
[14] *Id.*

NIST cannot allow any law enforcement concerns to override creation of the strongest available cryptography.

Other Provisions

In addition to the above, Access further commends NIST's commitment to including the public in its consultations on cryptographic standards. Specifically, requiring that public involvement be "meaningful" is a positive step toward inclusion of a multitude of views and opinions. However, we renew our call for IR 7977 to include a commitment to providing more transparency specifically around interactions with the NSA.

Thank you for this renewed opportunity to comment on the second draft of IR 7977. If you have any questions about our comments you can contact Amie Stepanovich, Access' U.S. Policy Manager, at amie@accessnow.org.

Respectfully Submitted,

Amie Stepanovich
Access U.S. Policy Manager

Drew Mitnick
Access Policy Counsel

Jack Bussell
Access Policy Intern

From: Tanja Lange [mailto:tanja@hyperelliptic.org]
Sent: Wednesday, April 08, 2015 2:32 AM
To: crypto-review
Subject: Comments on NISTIR 7977

Dear Ladies and Gentlemen,
Please find below my comments on NISTIR 7977. Sorry for the delay in submitting them. After speaking last week during PKC and the NIST workshop on post-quantum security to Sara Caswell and to Donna Dodson I hope you can still take my comments into account.

Best regards
Tanja Lange

Prof. Dr. Tanja Lange
Coding Theory and Cryptology, MF6.104 B
Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
P.O. Box 513
5600 MB Eindhoven
Netherlands

==========

Comments on "NIST Cryptographic Standards and Guidelines Development Process (Second Draft)", version of January 2015.

In general I was pleased with the efforts to update the IR. There are still some places which are ambiguous and should be fixed before the final version. This is giving the benefit of the doubt that these statements were underspecified by accident and not to leave open loopholes. The importance of this IR will depend on how how these gaps are filled in.

This updated draft starts with a detailed note to reviewers. I found this note very useful as it helped to clarify statements made before and to highlight the changes. Is this section going to stay? My best guess is no, because several parts appear later in the document. But the parts "Openness and transparency with public comments" and "Openness and transparency" appear only on p.3 and not later in the documents. Most parts are included but in a scattered manner; I strongly recommend copying these texts into the main body of the IR (with changes stated below) as individual entries. Handling of comments and attribution has been an major item of criticism in NIST's handling of SP80-90 and this deserves separate, easy to find entries.

Some detailed comments:

p.3,l.51 and l.54
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

p.4 How is NIST going to behave in the situation that some SDOs bring forward the same proposal/standard but researchers disagree with this selection. This case is not purely academic: the Chinese ZUC is accepted by CCSA and by ETSI Sage, yet does not enjoy much support from the academic community. Would this be a case of "When there is no community consensus and/or an existing standard, NIST will consider working with an SDO to develop a standard."?

p.14, l.374 "standards and guidelines are complementary" I hope they are also compatible.

p.14 l.379 The meetings between NIST and NSA seem an important place of information exchange and (possibly undue) influence on decisions. Are minutes of these meetings available? How is knowledge gained from these meeting attributed? How are the principles of openness and transparency applied to this information?

p.14 l.381 Do the 'other agencies' include the NSA? Please be specific on this touchy topic. Also please define what a 'significant contribution' is.

Footnote on p.14
"The names of some NSA staff cannot, by law, be publicly revealed. 50 U.S.C. §402 note. Freedom of Information Act (FOIA) requests for documents involving any NIST-NSA collaboration are normally reviewed by both organizations and exempted or excluded information, which may include the names of specific NSA participants as noted, may be redacted."
Interesting question: does this include undercover NSA staff? Would this mean that NSA undercover staff could make public comments which are then exempt from publication?

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.