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

April 18, 2014
Submitted via e-mail to crypto-review@nist.gov

On February 19, 2014, the National Institute of Standards and Technology ("NIST") published *NIST Cryptographic Standards and Guidelines Development Process (NIST IR 7977)*, a draft document that "outlines the principles, processes, and procedures of NIST's cryptographic standards efforts."[1] The draft document sets out key guiding principles and methods for engagement and outreach to ensure that adopted standards are "robust and have the confidence of the cryptographic community."[2]

On September 5, 2013, in joint reports by The Guardian,[3] The New York Times,[4] and ProPublica,[5] it was revealed that the National Security Agency ("NSA") had exerted influence over NIST in order to intentionally weaken NIST cryptographic standards. Under federal law, NIST is required to consult with NSA on the development of cryptographic standards.[6] One of NSA's primary missions is "information assurance," under which it "ensure[s] appropriate security solutions are in place to protect and defend information systems."[7] However, this mission is often at odds with NSA's other primary directive - signals intelligence, under which it conducts its communication surveillance activities. The President's Review Group on Intelligence and Communications Technologies has recommended significant structural changes to the NSA in order to separate these missions, but such separation has not yet occurred.[8]

[1] *NIST Cryptographic Standards and Guidelines Development Process (Draft),* NAT'L INST. OF SCI. AND TECH. (Feb. 2014), *available at* http://csrc.nist.gov/publications/drafts/nistir-7977/nistir_7977_draft.pdf [hereinafter NIST IR 7977].
[2] *Id.* at 1.
[3] James Ball, Julian Borger & Glenn Greenwald, *Revealed: How U.S. and U.K. Spy Agencies Defeat Internet Privacy and Security*, THE GUARDIAN, Sept. 5, 2013, *available at* http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.
[4] Nicole Perlroth, Jeff Larson & Scott Shane, *NSA Able to Foil Basic Safeguards of Privacy on Web,* N.Y. TIMES, Sept. 5, 2013, *available at* http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0.
[5] Jeff Larson, Nicole Perlroth & Scott Shane, *Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security*, PROPUBLICA, (Sept. 6, 2013), http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.
[6] *See* Federal Information Security Management Act of 2002 § 303(c), 44 U.S.C. § 3541; *see also* NIST IR 7977 at 2 ("NIST works closely with the NSA in the development of cryptographic standards. This is done because of the NSA's vast expertise in cryptography and because NIST, under the Federal Information Security Management Act of 2002, is statutorily required to consult with the NSA on standards.").
[7] *About IA. at NSA*, NAT'L SEC. AGENCY, http://www.nsa.gov/ia/ia_at_nsa/.
[8] The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, 21 (Dec. 12, 2013), *available at*

In regard to its conflicting missions, NSA's ability to wield influence over NIST remains central to the cryptography community's decreased confidence in the Agency. On September 10, 2013, NIST responded to the reports regarding the NSA:

> NIST has a long history of extensive collaboration with the world's cryptography experts to support robust encryption. The National Security Agency (NSA) participates in the NIST cryptography development process because of its recognized expertise. NIST is also required by statute to consult with the NSA. Recognizing community concern regarding some specific standards, we reopened the public comment period for Special Publication 800-90A and draft Special Publications 800-90B and 800-90C to give the public a second opportunity to view and comment on the standards.[9]

NIST has not publicly revealed to what extent or in what ways the NSA influenced these standards, or if evidence exists that other standards have been similarly undermined. In order to re-build confidence in NIST, it is necessary that the Agency takes pro-active steps toward implementing a more transparent, accountable process for standards development.

NIST IR 7977 sets out and elucidates guiding principles in the standards-setting process: transparency, openness, technical merit, balance, integrity, and continuous improvement. In order to meet NIST's goals, NIST guiding principles should be modified and amended to provide greater transparency and access. We address each of the six guiding principles in turn.

Transparency

Transparency is perhaps the area where NIST can best act to increase confidence in its internal processes and procedures. The draft document explains that NIST works toward transparency in its "selection and evaluation criteria, specification, security and performance characteristics, and provenance of proposed standards and guidelines."

In the development or adoption of standards, NIST should further commit, to the extent that it does not invade personal privacy interests, to transparency on the identity and affiliation of individuals and organizations that consult on the development process.

Specifically in regard to the NSA, NIST should establish a policy wherein the Agency publicly explains the extent and nature of the NSA's consultation on future standards and any modifications thereto made at NSA's request. Further, NIST should begin a review process to ensure that wherever possible the same information is published for standards that are currently

http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf ("NSA should be clearly designated as a foreign intelligence organization. Other missions (including that of NSA's Information Assurance Directorate) should generally be assigned elsewhere.").

[9] *Cryptographic Standards Statement*, NAT'L INST. OF SCI. AND TECH. (Sept. 10, 2013), http://www.nist.gov/director/cybersecuritystatement-091013.cfm.

in use. A full accounting of the interactions between the two Agencies will allow the cryptography community, oversight bodies, and the public at large to judge to what extent the NSA's signals intelligence mission is interfering with a process to develop the most secure standards.

Openness

NIST maintains a public-facing website on which it publishes its draft and final documents, standards, and other information. NIST also utilizes the Federal Register to publish documents on which a public comment opportunity is available. These sources are all used to create an open process.

Although not detailed in NIST IR 7977, NIST also maintains a Twitter account where information is often published and linked to, @USNISTgov.[10] The Twitter account was recently used during NIST's Privacy Engineering Workshop to "live-tweet" the panels and events of the event. For further example, the Office of the Director of National Intelligence recently launched a page on popular social networking website Tumblr to centralize the publication of information on national security issues.[11] The website has been generally well-received and considered a useful resource.

NIST should attempt to maximize reach and engagement and limit barriers to access in order to conduct the best possible outreach to the public. Formally embracing communication tools that allow for greater public outreach will put NIST on the forefront of online engagement and help ensure that interested parties are engaged in the NIST processes. In deciding on platforms, NIST should not only consider reach, level of engagement, and barriers to access, but also the ability to search for and access historical content to ensure persistence and continuity.

Technical Merit

While NIST may "strive[] to standardize cryptographic algorithms, schemes, and modes of operation whose security properties are well understood," it sometimes fails to provide the proper basis for external expert analysis. For example, prominent cryptography expert Matthew Green has highlighted how NIST's habit of not providing security proofs with its standards -- including the Dual_EC_DRBG standard suspected of having a backdoor[12] -- makes it more difficult for outside experts and stakeholders to evaluate the technical merits of the standards and participate in the standards process.[13] NIST should commit to always providing a security proof for standards when the standard is put out for public comment. NIST should also commit

[10] @usnistgov, https://www.twitter.com/usnistgov.
[11] IC ON THE RECORD, http://icontherecord.tumblr.com/.
[12] Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, & Hovav Shacham, *On the Practical Exploitability of Dual EC in TLS Implementations*, *available at* http://dualec.org/DualECTLS.pdf (last visited Apr. 18, 2014).
[13] Matthew Green, *The Many Flaws of Dual_EC*_DRBG, A FEW THOUGHTS ON CRYPTOGRAPHIC ENG'G (Sept. 18, 2013), http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html.

to explaining the justification for, origin, and means of generation for any parameters supplied in NIST standards.

Balance

The balance principle, under which NIST accepts input from all stakeholders to "ensure its standards...meet the needs of the federal government as well as the broader user community," should be narrowed. The provision should specify that, unless necessary, NIST will only take into account information assurance needs of government in establishing cryptography standards, and should, under no circumstances, consider the signals intelligence needs of the NSA or any other intelligence or law enforcement need of any agency.

Integrity

In Integrity, NIST explains that the Agency "serves as an impartial technical authority when developing cryptographic standards and guidelines."[14] However, as discussed above, NIST's requirement to consult with the NSA and the likelihood that the NSA has degraded certain standards calls this into question. In order to truly preserve the integrity of the Agency, NIST should act on the all of the recommendations in this document so that dealings with entities in the intelligence community are well-known and can be assessed in terms of their impact on a given standard.

Continuous Improvement

NIST's commitment to accepting expert feedback is commendable. The "open source" technique of inviting feedback to identified vulnerabilities is specifically in line with identified best practices.

In addition to these six guiding principles, NIST should also add a seventh – usability.

Usability

Even theoretically strong cryptography standards may be exploited in practice. In fact, "[u]ser errors cause or contribute to most computer security failures."[15] Cryptographer and programmer Daniel J. Bernstein has explained how standards that appear technically sound "when properly implemented and used for the purposes for which they…are designed," may still be extremely

[14] NIST IR 7977, *supra* note 1, at 2.

[15] Alma Whitten & J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0 in* IN SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE (eds. L. Cranor & G. Simson, O'Reilly, 2005) pp. 679-702, at 679, *available at* http://www.cs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf; *see also* Mike Hearn, Uability of Crypto Software (Mar. 5, 2014), Medium, https://medium.com/bitcoin-security-functionality/d04ea6a2c771 ("The security community has a problem, and we all know it. Too often, the people we wish were using our software can't figure it out.").

fragile and easy to use incorrectly.[16] Certain implementation errors may be anticipated or planned for such that it would render the implementation of a standard unsafe.[17]

In other industries, NIST has recognized usability, or “how easily someone can use [a product] for its intended purpose,” as a key consideration.[18] NIST should extend this to its cryptography work to ensure that security standards are not weaker in practice than anticipated by examining only the underlying mathematics.

NIST has traditionally served an important and unique role in the technical community. As Matthew Green has pointed out, “we’re highly dependent on NIST standards.”[19] If NIST is to continue to play this role, it needs to take drastic and affirmative actions to re-commit itself to its core mission and to remove any traces of impropriety.

Thank you for your request for public comment. We look forward to further engaging with NIST on this and other important matters.

Sincerely,

Access
Advocacy for Principled Action in Government
Competitive Enterprise Institute (“CEI”)
Electronic Frontier Foundation (“EFF”)
Electronic Privacy Information Center ("EPIC")
Fight for the Future
New America Foundation's Open Technology Institute
OpentheGovernment.org
Silent Circle
Student Net Alliance
Sunlight Foundation
TechFreedom

[16] Daniel J. Bernstein, How to Design an Elliptic-Curve Signature System (Mar. 23, 2014), The cr.yp.to blog, http://blog.cr.yp.to/20140323-ecdsa.html.
[17] *Id*.
[18] Press Release, NIST, NIST Releases Technical Guidance for Evaluating Electronic Health Records (Mar. 20, 2012), http://www.nist.gov/itl/iad/ehr-032012.cfm; *See also* NIST, Usability, http://www.nist.gov/healthcare/usability/ (last visited Apr. 18, 2014).
[19] Matthew Green, *On the NSA*, A FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING (Sept. 15, 2013), http://blog.cryptographyengineering.com/2013/09/on-nsa.html.