Recommendation for Random Number Generation Using Deterministic Random Bit Generators

In the Matter of

NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators	)))))	Re-opened Public Draft

October 2013
Comments of the
Internet Architecture Board
c/o Internet Society
1775 Wiehle Avenue, Suite 201
Reston, VA 20190-5108
Website: http://www.iab.org
Email: iab@iab.org

Recommendation for Random Number Generation Using Deterministic Random Bit Generators

In these comments, the Internet Architecture Board (IAB) responds to the re-opening of the comment period on SP 800-90 A[1], making recommendations relating to the review process for cybersecurity and cryptographic standards, in order to enhance transparency and openness.

The Transparency Imperative – Restoring Public Confidence

Within its standards, the Internet Engineering Task Force (IETF) has a long history of referencing NIST-approved cryptographic algorithms[2] as well as algorithms approved by other national governments[3] [4] [5]. News reports[6] questioning the integrity of NIST-approved cryptographic algorithms therefore raise grave concerns. IETF standards depend on NIST standards and the process by which they are developed. An open and transparent process is the only way to build confidence in the standards produced by any standards development organization, and NIST is no exception.

NIST has taken a major step toward transparency though support of the public comment process on draft documents, a step that is not yet common in the development of national cryptographic and cybersecurity standards. We also welcome the "Cryptographic Standards Statement"[7] in which it was stated that "If vulnerabilities are found in these or any other NIST standards, we will work with the cryptographic community to address them as quickly as possible."

However, re-running a process that previously yielded a questionable outcome may not be sufficient to restore public confidence. We therefore believe that more fundamental changes to the NIST review process should be considered, in order to improve transparency and openness and enable NIST to continue to be seen as an unbiased, trusted scientific venue for the development of cybersecurity and cryptographic standards. Specifically, the Internet Architecture Board (IAB) recommends that NIST:

---

[1] NIST, "NIST Opens Draft Special Publication 800-90A", September 2013, http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf

[2] Salter, M., Rescorla, E. and R. Housley, "Suite B Profile for Transport Layer Security (TLS)", RFC 5430, March 2009.

[3] Dolmatov, V., Chuprina, A. and I. Ustinov, "Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 6944, July 2010.

[4] Lee, H.J, Lee, S.J., Yoon, J.H., Cheon, D.H. and J.I. Lee, "The SEED Encryption Algorithm", RFC 4269, December 2005.

[5] Matsui, M., Nakajima, J. and S. Moriai, "Description of the Camelia Encryption Algorithm", RFC 3713, April 2004.

[6] Perlroth, N., Larson, J. and S. Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web", New York Times, September 5, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=1&

[7] NIST Office of the Director, "Cryptographic Standards Statement", September 10, 2013, http://www.nist.gov/director/cybersecuritystatement-091013.cfm

(a) Make publicly available on its Web site, in easily searchable form, all comments received (including the names of the authors and their affiliations), whether from sources inside the US or other governments, or from other parties;

(b) Provide for a reply comment period, so that reviewers can respond to comments made during the initial comment period;

(c) Provide a summary of comments received and their disposition;

(d) Provide a detailed and substantial explanation of changes resulting from internal review (even in cases where public comment was not initiated);

(e) Consider development of an appeals process.

We note that recommendations for improvements in the transparency and openness of NIST review processes have been made previously. For example, the Center for Regulatory Effectiveness (CRE) submitted a comment relating to recommendations (a), (b) and (c) during the review of SP 800-137[8]. We also note that these recommendations represent standard operating procedure for other US government agencies such as the Federal Communications Commission (FCC). Moreover, they are consistent with President Obama's Open Government Initiative[9].

We recognize that implementing a reply comment period is challenging without enforcing a rigid deadline for acceptance of comments, so that all received comments can be made available prior to the initiation of the reply comment period. With sufficient notice, we believe that commenters could adjust to a rigid deadline, and the benefits of enabling a reply comment period would compensate for the inconvenience.

In a recent blog post, the Center for Democracy and Technology (CDT) raised questions relating to the evolution of the SHA-3 standard[10] subsequent to issuance of the NIST third-round report on the SHA-3 algorithm competition[11]. This issue could be potentially addressed via recommendation (d).

Since a proposal to address recommendation (e) could take considerable time to develop, it should not be considered a pre-requisite for implementation of the other recommendations. Nevertheless, an appeals process represents an important component of due process which is likely to demonstrate its greatest value in times of controversy.

In closing, we believe that the current controversy provides an opportunity for NIST to adopt a more open and transparent standards development process. Such a process will increase confidence in cryptographic standards and the protocols that depend on them.

[8] The Center for Regulatory Effectiveness, Comment on NIST SP 800-137, March 2011, http://www.thecre.com/fisma/wp-content/uploads/2011/03/NIST-Comments-CRE-..1.pdf

[9] White House Open Government Initiative, http://www.whitehouse.gov/open

[10] Hall, Joseph Lorenzo, "What the heck is going on with NIST's cryptographic standards, SHA-3?", September 24, 2013, https://www.cdt.org/blogs/joseph-lorenzo-hall/2409-nist-sha-3

[11] NISTIR 7896, "Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition", November 2012, http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf