SUPPLEMENTAL ITL BULLETIN FOR SEPTEMBER 2013

NIST OPENS DRAFT SPECIAL PUBLICATION 800-90A, RECOMMENDATION FOR RANDOM NUMBER GENERATION USING DETERMINISTIC RANDOM BIT GENERATORS, FOR REVIEW AND COMMENT

The National Institute of Standards and Technology (NIST) first published specifications for random number generators (RNGs) in Federal Information Processing Standard (FIPS) 186-2, the Digital Signature Standard (DSS).

In 1998, NIST recognized that the random number generators described in FIPS 186-2 would not be adequate for anticipated future requirements for the generation of random numbers, and began an effort in conjunction with American Standards Committee (ASC) X9, the committee for Financial Services, to develop standards containing new methods for random number generation. The standard was designated as American National Standard (ANS) X9.82, *Random Number Generation*. ANS X9.82 consists of four parts: Part 1 is a general framework of the RNG process, Part 2 discusses entropy sources, Part 3 specifies Deterministic Random Bit Generators (DRBGs), and Part 4 specifies constructions for building Random Bit Generators (RBGs) using entropy sources that comply with Part 2 and DRBGs that comply with Part 3. Parts 1 and 3 have been completed and are available from ASC X9 (see http://www.x9.org). The comment period and ballot for Part 4 have been closed by the American National Standards Institute (ANSI).

In 2006, NIST published NIST Special Publication (SP) 800-90, Deterministic Random Bit Generators (DRBGs). This publication was later revised and became SP 800-90A in order to include additional publications on entropy sources and RBG constructions. SP 800-90/90A includes the DRBG specifications included in ANS X9.82. The entropy-source document (SP 800-90B) is currently under development, as is the RBG-construction document (SP 800-90C). The Federal government was the primary technical source for both the ANSI and NIST versions. Although these publications are nearly the same as the ANS X9.82 publications, NIST chose to publish the material as Special Publications to attract a broader set of experts within the cryptographic community. This is consistent with NIST's development procedures that are designed to attract comments from experts throughout the cryptographic community.

Concern has been expressed about one of the DRBG algorithms in SP 800-90/90A and ANS X9.82: the Dual Elliptic Curve Deterministic Random Bit Generation (Dual_EC_DRBG) algorithm. This algorithm includes default elliptic curve points for three elliptic curves, the provenance of which were not described. Security researchers have highlighted the importance of generating these elliptic curve points in a trustworthy way. This issue was identified during the development process, and the concern was initially addressed by including specifications for generating different points than the default values that were provided. However, recent community commentary has called into question the trustworthiness of these default elliptic curve points.

NIST works to publish the strongest cryptographic standards possible, and uses a transparent, public process to rigorously vet its standards and guidelines. If vulnerabilities are found, NIST works with the cryptographic community to address them as quickly as possible.

In light of the concerns expressed regarding Dual_EC_DRBG, ITL is taking the following actions:

Recommending against the use of SP 800-90A Dual Elliptic Curve Deterministic Random Bit Generation: NIST strongly recommends that, pending the resolution of the security concerns and the re-issuance of SP 800-90A, the Dual_EC_DRBG, as specified in the January 2012 version of SP 800-90A, no longer be used.

Re-issuing SP 800-90A as a draft for public comment: Effective immediately, NIST Special Publication 800-90A is being re-issued as a draft for public comment for a period ending November 6, 2013. Any concerns or recommendations for improvement regarding the *Recommendation for Random Number Generation Using Deterministic Random Bit* Generators are solicited (http://csrc.nist.gov/publications/PubsDrafts.html). NIST will review, analyze, and adjudicate all comments received during this 60 day period.

Reopening the Public Comment Period for SP 800-90B and 800-90C: NIST is reopening the drafts of SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation,* and SP 800-90C*, Recommendation for Random Bit Generator (RBG) Constructions,* for additional review, even though the documents have not been changed since their public review last year. The public comment period for these drafts will also close on November 6, 2013.

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.