The attached **DRAFT** document,

> **First Public Draft** NISTIR 7977, *NIST Cryptographic Standards and Guidelines Development Process, [February 2014]*

(**provided here for historical purposes**) has been superseded by the following draft publication:

Publication Number:	**SECOND PUBLIC DRAFT NISTIR 7977**
Title:	**NIST Cryptographic Standards and Guidelines Development Process**
Publication Date:	**January 23, 2015**

- Second Public Draft, January 2015: NISTIR 7977: *http://csrc.nist.gov/publications/drafts/nistir-7977/nistir_7977_second_draft.pdf*

- For information on the NIST Solicits Comments on its Cryptographic Standards Development Process **(NISTIR 7977 Second Public Draft (January 2015))** can be found at http://csrc.nist.gov/groups/ST/crypto-review/process.html

- For information on the NIST Solicits Comments on its Cryptographic Standards Development Process **(NISTIR 7977 First Public Draft [from the February 2014])** can be found at: http://csrc.nist.gov/groups/ST/crypto-review/process-feb2014.html

NISTIR 7977

NIST Cryptographic Standards and Guidelines Development Process (Draft)

The Cryptographic Technology Group

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 7977

NIST Cryptographic Standards and Guidelines Development Process (Draft)

The Cryptographic Technology Group
Information Technology Lab

February 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Interagency or Internal Report 7977
14 pages (February 2014)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *February 18, 2014* through *April 18, 2014*

National Institute of Standards and Technology

Attn: Computer Security Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Email: crypto-review@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

This document describes the principles, processes and procedures that drive our cryptographic standards development efforts. This draft document will be revised based on the feedback received during the public comment period, and the revised publication will serve as basis for NIST's future standards development efforts. It will also serve as the basis for the review of NIST's existing body of cryptographic standards and guidelines.

Keywords

Cryptographic standards; cryptographic guidelines;

Introduction

The Computer Security Division (CSD), a part of the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) is responsible for developing standards (i.e., Federal Information Processing Standards), guidelines (NIST Recommendations), tests, and metrics to protect non-national security federal information systems. Cryptographic standards and guidelines for the protection of sensitive federal information in transit or storage have always been a key component of this effort. These standards must be robust and have the confidence of the cryptographic community in order to be widely adopted and effective at securing information systems worldwide.

To ensure these standards provide high-quality, cost-effective security mechanisms, NIST works closely with a broad stakeholder community to select, define and promulgate these standards and guidelines. NIST's stakeholder community includes subject matter experts, academia, government agencies, and sectors and organizations that voluntarily adopt NIST cryptographic standards. NIST has found that open and transparent processes are critical to developing the most secure and trusted cryptographic standards possible. NIST strives to engage all of its stakeholders in these processes.

Principles

NIST believes equitable standards development processes produce the strongest, most effective, and most highly trusted cryptographic standards. The following principles guide NIST's standards and guidelines development processes.

Transparency: All interested and affected parties have access to essential information regarding standards-related activities and venues. NIST is committed to transparency in the development and documentation of its cryptographic standards with respect to the selection and evaluation criteria, specification, security and performance characteristics, and provenance of proposed standards or guidelines. NIST strives to be transparent with all stakeholders by informing and involving them through presentations at conferences and standards meetings, and publication of draft documents for public review.

Openness: Participation is open to all interested and affected parties. All stakeholders, including security professionals, researchers, standards development organizations, and users, have an opportunity to be involved in the standards and guidelines development process. NIST strives to maintain this open process by posting draft documents for public comment, holding public workshops and conferences, and engaging the cryptographic community at industry and academic events.

Technical Merit: NIST's decisions during the development of cryptographic standards and guidelines are based on the technical merit of a proposal. NIST strives to standardize cryptographic algorithms, schemes, and modes of operation whose security properties are well understood.

Balance: NIST strives to achieve balance of interests among stakeholders, weighing these interests to develop cryptographic standards that are secure, efficient, and promote interoperability. NIST solicits input from a wide-range of stakeholders representing government, industry and academia to ensure its standards are strong, practical, and meet the needs of the Federal government as well as the broader user community.

Integrity: NIST serves as an impartial technical authority when developing cryptographic standards and guidelines. When evaluating, selecting, and standardizing cryptographic algorithms, NIST strives to maintain its objectivity when it forms and documents its decisions.***Continuous Improvement:*** During the course of the development of cryptographic algorithms, the cryptographic community is encouraged to identify weaknesses, vulnerabilities, or other deficiencies in cryptographic functions specified in NIST publications. When vulnerabilities are identified, NIST engages with the broader cryptographic community to address them.

Stakeholders

NIST's statutory responsibility is to develop cryptographic standards and guidelines for protecting sensitive government information on non-national security systems. These are widely used across the federal government. However, NIST cryptographic standards have long been voluntarily adopted by other public and private organizations. For example, the Data Encryption Standard (DES), published as Federal Information Processing Standard (FIPS) 46 in 1977, filled a critical need for the financial services industry at a time when electronic transactions were becoming commonplace. NIST cryptographic standards and guidelines continue to be voluntarily adopted in the private sector, particularly in the financial and health care sectors.

The national security community within the United States federal government has also adopted a subset of NIST's cryptographic standards and guidelines through the Suite B program. The NIST algorithms that comprise Suite B have been approved by the National Security Agency (NSA) to protect classified information up to the Secret level, with a class of algorithms with larger key sizes approved to protect information at the Top Secret level. 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.

Standards Developing Organizations (SDOs) have also adopted NIST cryptographic standards as foundational building blocks for security protocols. For example, the Advanced Encryption Standard (AES) block cipher is included in ISO/IEC 18033-3:2010, is the preferred block cipher for IEEE 802.11 to secure wireless networks, and is mandatory to implement in version 1.2 of the IETF's Transport Layer Security (TLS) protocol.

This widespread adoption has had significant benefits for all participating communities, whether they are participating by statute or by choice. Widespread international adoption has resulted in widespread availability of commercial products supporting strong cryptography. In combination with international standards, security services that are globally interoperable have permitted an explosion of e-commerce internationally.

NIST works closely with experts in industry, academia and government to develop its cryptographic standards and guidelines. Since the development of DES, the community researching and developing cryptographic technologies within industry and academia has expanded greatly. Using the mechanisms and processes described in this document, NIST works with these stakeholders to identify areas where standards or guidelines are needed, evaluate proposals, and develop standards or publications. NIST's role as a well-respected and trusted technical authority in this field is to balance these needs to ensure that its standards and guidelines are technically sound and have the confidence of the community.

Engaging the Cryptographic Community

NIST uses a variety of mechanisms to engage its stakeholders in academia, industry, and government in the development of its cryptographic standards and guidelines. These mechanisms include holding international competitions to select new cryptographic algorithms, participating in SDOs, and developing new standards in collaboration with cryptographers around the world.

Cryptographic Competitions

Cryptographic algorithm competitions allow NIST to standardize a state-of-the-art, widely accepted cryptographic primitive by involving the international cryptographic research community in a fair, open-design competition to select an algorithm that NIST will standardize and promote. Interested parties have an opportunity to participate in the competition by publishing research papers, submitting comments, and attending public workshops. Researchers contribute candidate designs and papers on theory, cryptanalysis and performance. The winning submitters are recognized, but agree to relinquish claim to intellectual property rights for their design so that the winning candidate can be available for royalty-free use. NIST determines the algorithm submission requirements and selection criteria, organizes workshops, hosts a competition website and e-mail discussion forum, selects the winning algorithm (based on its own analysis and that of the public), and explains and documents the selection.

A typical competition starts with a public dialog on the need and requirements for a new algorithm, both on-line and through public workshop(s), as well as a Federal Register announcement inviting comment on NIST's proposed criteria. A subsequent Federal Register announcement states the submission requirements, schedule and selection criteria. A candidate conference is held, usually juxtaposed with a major cryptographic research conference, for each "round" of the competition to review the candidates and research results (i.e., cryptanalysis, performance and proofs of properties) on the candidates. Following each round, NIST announces the candidates selected to continue to the next round, and provides a report that documents the rationale for the selections. This winnowing allows the community to focus its analytical efforts on the most promising candidates. The last round usually has about five strong candidates. Following the final candidate conference, NIST selects the winner, writes a final report and formally proposes a standard for the algorithm through the normal FIPS process.

Adoption of Existing Standards

NIST participates in Standards Development Organizations (SDOs), either as a member organization (e.g., X9, Inc.[1] working groups, INCITS[2] technical committees), or as individual representatives (e.g., IEEE SA[3] working groups and IETF[4] working groups). NIST experts also participate in some international SDOs through US National Body or Member State representation. ANSI[5] is the sole US representative for two major non-treaty international standards organizations, the International Organization for Standardization (ISO), and, via the US National Committee (USNC), the International Electrotechnical Commission (IEC). For treaty-based international standards bodies, such as the International Telecommunication Union (ITU), the Department of State represents the US.

The principles used to develop voluntary consensus standards within SDOs are outlined in OMB Circular A-119, which instructs agencies to consider the use of these standards except where inconsistent with law or otherwise impractical. Active participation in such SDOs helps to ensure that NIST cryptographic standards and guidelines are highly secure and interoperable with its international partners. When appropriate, SDO publications are referenced in NIST guidance publications.

Development of New Standards

When NIST identifies a requirement for a standard and determines that no suitable standard already exists, NIST often develops a guidance document for use by Federal agencies. If there is also broader applicability, NIST may offer the guidance document or an adaptation of the document as a contribution to an SDO standards activity. NIST experts in cryptographic algorithms and standards develop these guidance documents in collaboration with experts in academia, industry and government. Transparency and collaboration is accomplished through formal public review processes and interaction with experts at public workshops and standards meetings. For the development of new, basic cryptographic functions, NIST may invite contributions from the public and hold a formal competition. In some cases, NIST guidance publications are offered as contributions to and form a basis for SDO standards.

NIST Publications

NIST uses several types of documents to publish and disseminate its cryptographic standards and guidelines. Three categories of NIST publications are commonly used: Federal Information Processing Standards, Special Publications, and Interagency Reports. Draft and final cryptographic standards and guidelines are posted by NIST on its Computer Security Resource Center web pages and are freely available to anyone.

---

[1] X9, Inc., Financial Industry Standards.
[2] InterNational Committee for Information Technology Standards.
[3] Institute of Electronic and Electrical Engineers Standards Association.
[4] Internet Engineering Task Force.
[5] American National Standards Institute.

Federal Information Processing Standards (FIPS): FIPS publications are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347). FIPS publications are used by NIST to publish standards for fundamental cryptographic primitives, such as block ciphers, digital signature algorithms, and hash functions.

Special Publications (800 Series): The Special Publication 800 series document a wide range of research, guidelines, and outreach efforts in computer security. Cryptographic guidelines in the 800 series build upon the primitives specified in FIPS publications, sometimes specifying additional cryptographic algorithms, schemes and modes of operation, as well as providing guidance for their use. For example, Special Publications in the 800 series specify random bit generators, block cipher modes of operation, key-derivation functions, and key-establishment schemes. These algorithms and schemes use the block ciphers, hash functions, and mathematical primitives defined in FIPS publications as fundamental building blocks. In addition, NIST also issues guidelines on the selection and use of cryptographic algorithms in 800 series Special Publications.

NIST Interagency Reports (NIST IR): NIST IRs describe technical research of interest to a specialized audience. NIST does not specify cryptographic algorithms in NIST IR publications. Instead, NIST uses NIST IR publications to disseminate information about its cryptographic standards efforts. Historically, the Computer Security Division has used NIST IRs to publish workshop and conference reports, discussion documents on new challenges in cryptography, and status reports on cryptographic algorithm competitions.

While any NIST publication containing cryptographic standards or guidelines is first released as a draft for public comment, the specific development process differs by publication type. Because FIPS are mandated by formal legislation, and the algorithms they specify are at the heart of many critical security technologies, FIPS publications undergo the most formal development process. FIPS documents are developed by NIST, but approved and promulgated by the Secretary of Commerce. Formal announcements for draft and final FIPS documents are published in the Federal Register. As such, FIPS documents tend to have much longer development cycles than Special Publications. Special Publications are promulgated by NIST, with announcements posted on the Computer Security Division website. Special Publications have a shorter development cycle and usually are not announced in the Federal Register but are posted for a specified public comment period for external review and participation.

Public Review and Outreach

NIST strives in its cryptographic standards and guidance activities to be as open, and transparent as possible. NIST provides public notice of its activities in cryptography including:

- Plans for cryptographic standards and recommendations,
- Invitations for public participation in workshops that discuss topics in cryptography and its standardization,

- Announcements of the availability of draft cryptographic standards and recommendations for public review and comment, and
- Announcements of the adoption of cryptographic standards and recommendations for use by the US Federal Government.

All announcements are posted and available on the Computer Security Division website (http://csrc.nist.gov), while major announcements, including those proposing the adoption of FIPS and inviting comments on a proposed standard, are also announced in the Federal Register. In addition, press releases usually accompany significant announcements, and sometimes Information Technology Laboratory (ITL) Security Bulletins are posted that provide information about the use of cryptographic standards and recommendations. In some cases, NIST maintains a public email forum for ongoing open discussion of subjects relevant to cryptographic standards or research activities.

The primary feedback mechanism for NIST cryptographic designs and implementation guidance is the posting of drafts and requests for public comment on the Computer Security Division website. Comment periods depend on the size and complexity of the drafts, as well as any prior history of public exposure and commentary, but typically run from 30 to 90 days. Comments may be submitted as electronic mail messages, transmission of electronically completed comment templates, or as hard copy correspondence. If the nature or extent of changes to a draft resulting from the comments is sufficiently extensive, one or more additional cycles of public review may be conducted. Comments received on draft FIPS, and their dispositions, are summarized in the Federal Register Notice announcing the approval of a new or revised standard. In the case of commercial or consensus standards, feedback is generated and received in accordance with the policies and procedures of the respective standards bodies.

Announcements and public review are vital, but only the externally visible part of the process. Public outreach begins well before formal announcements and extends beyond the adoption of standards. NIST is deeply involved in the cryptographic research community, participating extensively in the community by attending research conferences; providing program committee members, speakers and reviewers for conferences and workshops; and writing papers on NIST research. NIST also invites and hosts guest researchers, postdoctoral fellows and visiting scholars; sometimes funds academic research; and provides services, such as the NIST Randomness Beacon,[6] for the research community. As a result, cryptographers around the world often know whom to contact at NIST in their area of interest. NIST encourages and receives valuable informal advice, often based on independent cryptanalysis, from researchers.

NIST's previously discussed participation in SDOs provides another avenue for outreach and feedback. In many cases, NIST staff are contributors, editors or working-group chairs for proposed voluntary standards that use cryptography. NIST participates in the SDO standards process along with industry and companies involved in the design, development and implementation of cryptography. Such outreach promotes a two-way flow of information, and provides early feedback on the effects of NIST standards and the need for new or different standards.

[6] See http://www.nist.gov/itl/csd/ct/nist_beacon.cfm

NIST must prioritize its participation within meetings, conferences, standards organizations and industry groups based on the stakeholders involved and the expected impact of involvement. There are also limits on the number of guest researchers and visiting scholars that can be accommodated, based on the available resources. Process and fairness require that some activities be kept confidential until announced publicly to everyone at the same time. Within these constraints, NIST strives to keep stakeholders informed by reaching out to the community, being accessible for discussions, listening to concerns, responding to questions, making important activities public, participating actively in the cryptographic research community, and supporting voluntary standards development efforts.

Appendix: Examples of Development Processes

Advanced Encryption Standard

During the 1990s, NIST wanted a block cipher standard that was stronger and faster than the existing Triple-DES standard, which was primarily used for encryption and message authentication. In January 1997 NIST announced its interest in the development of a successor to Triple-DES, to be called the Advanced Encryption Standard (AES). NIST requested feedback and held a public workshop to discuss the criteria for the design of this algorithm. NIST then announced the start of a competition and its rules and requirements in September 1997, calling for candidate submissions in nine months. NIST received 15 complete candidates, and held three conferences to review and winnow the candidates down to five finalists. After the third conference, NIST chose Rijndael to be the AES in October 2000, and in February 2001, formally proposed the AES standard, FIPS 197, in a Federal Register announcement soliciting public comment. The final approval of AES occurred on November 26, 2001.

Block Cipher Modes of Operation

FIPS 197 authorizes NIST Recommendations as a source for modes of operation for implementations of the AES algorithm. Recommendations for a variety of modes have been published, in a relatively agile manner under that authority, in the 800-38 series of Special Publications. Two sets of those modes originated in the Federal government: 1) the adaptations of the four DES encryption modes in FIPS 81 to the AES algorithm, and 2) the key-wrapping modes that were developed by NSA at NIST's request. All of the other block cipher modes approved by NIST were based on proposals that were submitted for NIST's consideration from academia and industry, including both individual companies and standards groups. All mode proposals are posted on NIST's CSRC website, with an open invitation for public comments.

The initial step in the development process is to determine whether a version of a mode proposal is appropriate to include in NIST's cryptographic toolkit of standards. The main considerations are: 1) whether the mode serves an important need, 2) whether existing modes in the toolkit, or other modes proposals, can adequately provide the needed properties/functionality, 3) whether the mode meets NIST's security requirements, and 4) for patented modes, whether acceptable royalty-free alternatives are available. NIST has often sought public input into these initial decisions, either from public workshops or through public comment periods.

When NIST is interested in approving a mode proposal, the next step is the development of a draft special publication that specifies the mode. Normally, NIST develops the draft in consultation with the mode submitter. After passing internal review, the draft is posted on the CSRC website for a period of public comment, after which any received comments are also posted. NIST considers the public comments carefully and decides

whether to finalize the draft for publication, with appropriate revisions to address any remaining public or internal concerns.

Since 2001, NIST has approved twelve block cipher modes of operation within six special publications in the 800-38 series. These modes provide confidentiality and/or authentication for a variety of general and special purpose applications, including modes designed for wireless local-area networks, disk encryption, and high-throughput Internet routers. A seventh document in the series, specifying modes for format-preserving encryption, is currently in development.

Deterministic Random Bit Generators

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. As a member of X9F1, a subcommittee of the American Standards Committee (ASC) X9 (the committee for Financial Services), NIST concluded that X9F1 would be an appropriate venue to develop a standard on random number generation, since the committee included members from several organizations with cryptographic expertise. A development team was formed to develop this standard (ANS X9.82) led by NIST and NSA staff. The standard was developed in four parts: a general discussion of random number generators (Part 1), requirements for entropy sources (Part 2), specifications for deterministic random bit generator (DRBG) algorithms (Part 3), and constructions for building Random Bit Generators (RBGs) from DRBGs and entropy sources (Part 4).

During the development of Part 3 of ANS X9.82, a version of the document was provided to the International Standards Organization (ISO), where it became the basis for ISO/IEC 18031.

In order to obtain a wider review of the standard, include additional test and validation guidance that was not appropriate for the X9 standard, and allow a more efficient review and comment process, NIST incorporated the material into the SP 800-90 series of documents. This series specifies algorithms (in NIST SP 800-90A), requirements and tests for entropy sources (in NIST SP 800-90B), and constructions for combining the DRBG algorithms and entropy sources into Random Bit Generators (in NIST SP 800-90C).

ANS X9.82, Part 3 became the basis for NIST SP800-90A. Part 3 of ANS X9.82 contains three algorithms: *HMAC_DRBG*, *CTR_DRBG* and *Dual_EC_DRBG*. However, when SP 800-90A was developed, four algorithms were included: *Hash_DRBG*, *HMAC_DRBG*, *CTR_DRBG* and *Dual_EC_DRBG*. *Hash_DRBG* was originally designed in response to a request for a generator that would be appropriate for the generation of values with higher security requirements than were provided in the older random number generators specified in the Digital Signature Standard (FIPS 186-2).

During the development of the SP 800-90 series, NIST has held several workshops, hosted discussions with organizations and experts involved in testing or designing

random bit generators, and provided the drafts of the SP 800-90 documents for public comment. All such feedback was considered for incorporation into the SP 800-90 documents.

Some in the cryptographic community have expressed concern about the *Dual_EC_DRBG* specified in SP 800-90A. In light of these concerns, NIST published an ITL Bulletin[7] discussing the history of the document development and the issue of concern, provided the SP 800-90 documents for an additional public comment period, and advised against using the *Dual_EC_DRBG* pending the resolution of the security concerns. As part of our commitment to continuous improvement of our standards and guidelines, NIST will review these comments and make a determination of the appropriate action to take.

[7] See http://csrc.nist.gov/publications/nistbul