NISTIR 7977

NIST Cryptographic Standards and Guidelines Development Process (Second 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 (Second Draft)

Cryptographic Technology Group
Computer Security Division
Information Technology Laboratory

January 2015



U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie E. May, Acting Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Interagency Report 7977
29 pages (January 2015)

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: January 23, 2015 through March 27, 2015

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 cryptographic standards and guidelines development efforts at the National Institute of Standards and Technology. This draft document reflects public comments received on an earlier version. It will be revised based on the feedback received during the public comment period, and the final publication will serve as the basis to guide NIST's future cryptographic standards and guidelines development efforts.

Keywords

Cryptographic standards; cryptographic guidelines; cryptographic research

Table of Contents

Note to Reviewers 2

Introduction and Overview 6

Principles 7

Publications for NIST's Cryptographic Standards and Guidelines 9

Engaging the Cryptographic Community 12

Public Notice and Review of Proposed and Final Standards and Guidelines 18

Policies and Processes for the Life Cycle Management of Cryptographic Standards and Guidelines 20

Note to Reviewers

> "It is of paramount importance that NIST's process for developing cryptographic standards is open and transparent and has the trust and support of the cryptographic community. This includes improving the discipline required in carefully and openly documenting such developments."
>
> *Report of the NIST Visiting Committee on Advanced Technology, July 2014*

After concerns were raised by the cryptographic community about the integrity of NIST's cryptographic standards and guidelines in November 2013, NIST initiated an internal review of its development process and announced it would seek public input and an independent review. Based on the February 2014 draft of this publication describing NIST's approaches and processes (NISTIR 7977, *NIST Cryptographic Standards and Guidelines Development Process*), multiple stakeholders provided recommendations. Commenters included experts tasked by NIST's top-level advisory committee as well diverse members of the global cryptographic and standards development community.

After considering all input, NIST is making several changes to its approaches and processes and clarifying others. These modifications are reflected in this revised version of NISTIR 7977, which is being made available for public review to request additional stakeholder input. Key changes include:

Additions and clarifications of principles to guide and govern NIST's work on cryptographic standards and guidelines

NIST is adding the following principles and steps:

- *Usability*. This principle is intended to clarify that NIST cryptographic standards and guidelines are designed and selected to help implementers create secure and usable systems for their customers that support business needs and workflows, and to be readily integrated with existing and future schemes and systems.
- *Innovation and Intellectual Property (IP).* NIST seeks to incentivize innovation while protecting IP in the field of cryptography. Noting a strong preference among its stakeholders for solutions that are unencumbered by royalty-bearing patented technologies, NIST prefers to select unencumbered cryptographic algorithms. NIST may also select encumbered algorithms (those with patent protections) if the technical benefits outweigh the negative implications.

NIST is clarifying principles and steps:

- *Balance, transparency, openness and integrity*. While being aware of law enforcement and national security concerns, NIST focuses on its mission of developing strong cryptographic standards for meeting U.S. federal agency non-national security and commerce needs. In order to make independent decisions, NIST stresses the importance of its access to sufficient expertise, both from within NIST and from organizations and individuals external to NIST.
- O*penness* and *transparency with public comments.* NIST will accept and make public all comments on draft standards and guidelines, in accordance with applicable law.
- *Openness and transparency.* As a general policy, NIST will release any available significant analyses and evaluations of algorithms or schemes included in NIST's cryptographic standards or guidelines, in accordance with applicable law. Moreover, NIST will pursue security proofs in the development of its cryptographic standards and guidelines, and encourage their development and analysis by the research community. In solicitations for proposed algorithms, NIST will ask for these proofs and, when available, include them in the public record when standards and guidelines are developed.
- *Integrity.* This principle encompasses the avoidance and appropriate management of conflicts of interest in the standards development process. NIST follows procedures to manage the risk presented by those conflicts and ensures appropriate training for its staff.
- *Technical merit.* This principle highlights the importance of ensuring that cryptographic standards and guidelines are based on algorithms, schemes and protocols that are secure, well-understood, efficient, and robust against accidental misuse, and that promote interoperability.

Formal Policies and Processes for the Life Cycle of Cryptographic Standards and Guidelines

NIST is describing more formal policies and processes for the life cycle management of cryptographic standards and guidelines – from the initial selection of areas to be addressed through the development, solicitation and response to comments and recommendations, consideration by Standards Developing Organizations (SDOs), and regular maintenance and review. Among other things, these policies and processes include provisions to:

- Indicate why NIST has selected a particular approach (e.g., adopt widely accepted standard, work with SDOs in developing a new standard, develop a new NIST standard or guideline, or hold an open competition) when establishing standards and guidelines.
- Announce NIST's plans when producing standards or guidelines and indicate a timeframe for reviewing and maintaining those documents – including updating and possibly withdrawing the document.
- Disclose all comments on drafts in accordance with applicable law.

- Create more systematic and transparent record-keeping policies and procedures.
- NIST will consider the use of open competitions to establish cryptographic standards particularly when no consensus exists yet around the best algorithmic approach. Competitions work best when a proposed algorithm or scheme requires a great deal of new cryptanalysis, as these competitions can focus the attention of cryptographers around the world. Decisions to use competitions will be made while recognizing and considering that these competitions are lengthy and resource intensive.

Interactions with Standards Developing Organizations

NIST is clarifying its role in working with SDOs and its policies regarding the consideration of SDOs' standards and standards development capabilities. This includes provisions to:

- Explicitly acknowledge the role and importance of SDOs, including international SDOs, in the development and acceptance of cryptographic standards. Vigorous and documented participatory processes are important in considering SDOs' work in this arena.
- Pursue a global acceptance strategy for NIST's cryptographic standards, including aiming to prioritize resources to support this strategy.
- Select voluntary consensus standards if NIST's objectives can be achieved by doing so (following OMB Circular A-119). When there is no community consensus and/or an existing standard, NIST will consider working with an SDO to develop a standard. If that is not a viable option, NIST will develop its own standard and give strong consideration to submitting this standard to an SDO.
- Clarify the role of NIST: 1) as a developer of standards and guidelines under statute for use in federal government non-national security information systems, noting that these often provide value to a broader set of stakeholders in U.S. and international business and commerce, and 2) as a technical contributor and stakeholder in connection with voluntary, global standards development.
- Prioritize which NIST standards and guidelines are brought to SDOs, based on likely impact and need and industry interest.
- Clarify the roles of NIST staff in working with SDOs, including stating the basis for determining NIST's participation. NIST affirms that its parameters for participation include ensuring that potential conflicts of interest are addressed.

Strengthening NIST's Cryptographic Capabilities

Recognizing that NIST increasingly must support the research needed to advance the science and lay the foundation for future cryptographic standards – to the extent that resources permit – the revised draft NISTIR states that NIST intends to participate extensively in the community by:

- Taking part in the work of SDOs;
- Preparing papers on NIST research and presenting at and attending research conferences;
- Providing additional program committee members, speakers and reviewers for conferences and workshops;
- Increasing invitations to host guest researchers, postdoctoral fellows and visiting scholars; and
- Increasing funding for both external (including academic) and internal research.

Notably, funding for NIST's work in cryptography-related programs has been expanded significantly with the enactment of appropriations for Fiscal Year 2015 operations of the Federal government. This increase will support internal as well as external efforts related to NIST's cryptographic standards and guidelines.

Comments Requested on This Revised Draft

As part of the public review of this revised draft, NIST requests comments on the following topics:

- Do the expanded and revised principles state appropriate drivers and conditions for NIST's efforts related to cryptographic standards and guidelines?
- 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?
- 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?
- Are there other channels or mechanisms that NIST should consider in order to communicate most effectively with its stakeholders?

Introduction and Overview

The National Institute of Standards and Technology (NIST) is responsible for developing standards (Federal Information Processing Standards, or "FIPS") and guidelines to protect non-national security federal information systems. Outside the Federal Government, these publications are voluntarily relied upon across many sectors to promote economic development and protect sensitive personal and corporate information. NIST has a dual role in this regard: 1) as a developer of standards and guidelines under federal law, and 2) as a technical contributor and stakeholder in connection with voluntary, global standards development. NIST has authority to conduct these activities under 15 U.S.C. 278g-3 and 15 U.S.C. 272(b)(3) and (b)(10).

The Computer Security Division (CSD), a part of the NIST Information Technology Laboratory (ITL), is charged with carrying out these responsibilities. Cryptographic standards and guidelines for the protection of federal information systems have always been a key component of this effort. They 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 and guidelines provide high quality, cost-effective security mechanisms, NIST works closely with a broad stakeholder community to identify areas of need and develop standards and guidelines. That community has expanded in recent years and now is truly global in nature, as is the interest in having a system in place that will appropriately protect and ensure the security of digitized information. That community includes experts from academia and government agencies, and from sectors and organizations that choose to adopt NIST cryptographic standards and guidelines. NIST knows – and has been reminded by stakeholders – 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, and has strengthened its efforts. This document sets forth the principles and processes NIST will use for future cryptographic standards and guidelines and reflects substantial stakeholder input.

It is vital that NIST has access to the most recent and relevant expertise regarding cryptography wherever this expertise resides. NIST must employ staff capable of soliciting, analyzing, and putting this cryptographic knowledge to use in developing standards and guidelines, tests, and metrics. In order to carry out its mission of protecting information and information systems, NIST also needs to be actively involved in advancing the field of cryptography. NIST is committed to achieving these goals by ensuring that its internal capabilities are strong and effective, and that it has robust access to external expertise. The agency's research investment in the cryptographic arena helps to ensure that the algorithms and schemes in its standards and guidelines are secure. This research also aids in building the foundation for standards and guidelines, whether they are developed by NIST or by other organizations.

Principles

NIST believes that robust, widely understood, and participatory development processes produce the strongest, most effective, most trusted, and broadly accepted cryptographic standards and guidelines. The following eight principles guide NIST's cryptographic standards and guidelines development processes.

Transparency: All interested and affected parties have access to essential information regarding standards and guidelines-related activities throughout the development process. NIST is committed to transparency in the development and documentation of its cryptographic standards with respect to the areas of focus, selection and evaluation criteria, specifications, security and other performance characteristics, and provenance.

Openness: Participation is open to all interested parties. All stakeholders – including security professionals, researchers, SDOs, and users – have an opportunity to be meaningfully involved in the standards and guidelines development process.

Technical Merit: NIST's decisions during the development of cryptographic standards and guidelines are based on the technical merit of a proposal while being mindful of security, privacy, policy and business considerations. NIST strives to standardize secure cryptographic algorithms, schemes, and modes of operation whose security properties are well understood, and are efficient, robust against accidental misuse, and promote interoperability. The review of technical merit includes a precise, formal statement of security claims, based on minimal security assumptions and supported as far as possible by documented cryptanalysis and security reduction proofs.

Usability: NIST aims to develop cryptographic standards and guidelines that help implementers create secure and usable systems for their customers that support business needs and workflows, and can be readily integrated with existing and future schemes and systems. Cryptographic standards and guidelines should be chosen to minimize the demands on users and implementers as well as the adverse consequences of human mistakes and equipment failures.

Balance: NIST strives to achieve a balance of interests among stakeholders, weighing these interests to develop cryptographic standards and guidelines that are secure, efficient, and promote interoperability. NIST solicits input from a wide range of stakeholders representing government, industry and academia to ensure that its standards are strong, practical, and meet the needs of the Federal Government as well as the broader user community. While being aware of implications related to law enforcement and national security, NIST focuses on its mission of developing strong cryptographic standards and guidelines for meeting U.S. federal agency and commerce needs.

Integrity: NIST serves as an impartial technical authority when it is developing cryptographic standards and guidelines. When evaluating, selecting, and standardizing cryptographic algorithms, NIST strives to maintain objectivity as it forms and documents its decisions. NIST will conduct its standards selection and development processes with clear criteria, and guard against undue or improper influence while considering the legitimate interests of stakeholders. NIST will never knowingly misrepresent or conceal security proprieties.

Continuous Improvement: As cryptographic algorithms are developed, and for the duration of their use, the cryptographic community is encouraged to identify weaknesses, vulnerabilities, or other deficiencies in the algorithms specified in NIST publications. When serious problems are identified, NIST engages with the broader cryptographic community to address them. NIST conducts research in order to stay current, to enable new cryptographic advances that may affect the suitability of standards and guidelines, and so that NIST and others can take advantage of those advances to strengthen standards and guidelines.

Innovation and Intellectual Property (IP): While developing its cryptographic standards and guidelines for non-national security systems, NIST has noted a strong preference among its users for solutions that are unencumbered by royalty-bearing patented technologies. NIST has observed that widespread adoption of cryptographic solutions that it has developed has been facilitated by royalty-free licensing terms. While NIST prefers to select unencumbered algorithms, it may select algorithms with associated patents if the technical benefits outweigh the potential costs that would be incurred in implementing the patented technologies. NIST will explicitly recognize and respect the value of IP and the need to protect IP if it is incorporated into standards or guidelines. Furthermore, NIST believes it is important to balance the rights of IP holders and of those seeking to utilize technologies involving intellectual property rights.

Publications for NIST's Cryptographic Standards and Guidelines

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, NIST Special Publications, and NIST Interagency Reports. Draft and final cryptographic standards and guidelines are posted by NIST on its Computer Security Resource Center web pages (http://www.csrc.nist.gov) and are freely available to everyone.

Federal Information Processing Standards (FIPS): By federal statute[1], FIPS publications are issued by NIST after approval by the Secretary of Commerce. They are used by NIST to publish standards for fundamental cryptographic primitives, such as block ciphers, digital signature algorithms, and hash functions.

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

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

All NIST publications containing cryptographic standards or guidelines are first released as a draft for public comment, although the development process differs by publication type. Because FIPS are mandated by statute and the algorithms they specify are at the heart of many critical security technologies, they require the most formal development process. Developed by NIST, FIPS are approved and promulgated by the Secretary of Commerce. Formal announcements for draft and final FIPS are published in the *Federal Register.* In part due to this development process, FIPS tend to have relatively long development cycles. SPs are promulgated by NIST,

[1] 15 U.S.C. 278g-3, as amended.

with announcements posted on the CSD website (http://csrc.nist.gov) rather than in the *Federal Register*, and may have a shorter development cycle. The same holds true for most of the computer security-related NISTIRs published by NIST.

Stakeholders for NIST's Cryptographic Standards and Guidelines

NIST is statutorily responsible for developing cryptographic standards and guidelines for the protection of information on non-national security systems that are used widely across the Federal Government. Additionally, the President occasionally issues Presidential Directives that direct NIST to develop specific standards or guidelines. Therefore, U.S. Government agencies and their suppliers and users are primary stakeholders for this work.

In addition, NIST cryptographic standards have long been adopted voluntarily by other public and private organizations and have significant, positive impacts on U.S. businesses and commerce and the broader global economy. For example, the Data Encryption Standard (DES), published as FIPS 46 in 1977, filled a critical need for the financial services industry – through its adoption as American National Standard X3.92 in 1981 – at a time when electronic transactions were becoming commonplace. NIST cryptographic standards and guidelines continue to be widely used voluntarily in the private sector, particularly in the financial and health care sectors. Consequently, NIST considers its stakeholder community for cryptographic standards, guidelines, tools and metrics to be much broader than those entities focused strictly on protecting government information on non-national security systems.

The national security community within the U.S. Federal Government has also adopted a subset of NIST's cryptographic standards and guidelines through the Suite B program. The National Security Agency (NSA) has approved the algorithms that comprise Suite B 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. Because of the national security sector's use of NIST cryptographic standards and guidelines, that sector is also an important stakeholder.

Widespread adoption of cryptographic standards has had significant benefits for all participating communities, whether they do so by statute or voluntarily. International adoption has resulted in widely available commercial products that support strong cryptography. In combination with these international standards, security services that are globally interoperable have facilitated the rapid expansion of global e-commerce. With increasing awareness of the risks associated with the use of the Internet, ready access to strong, reliable cryptography that is accepted globally has become even more important for stakeholders throughout the world.

Engaging the Cryptographic Community

NIST works closely with experts in industry, academia and government to develop its cryptographic standards and guidelines. Since the development of DES in the 1970s, the community researching and developing cryptographic technologies within industry and academia has expanded dramatically.

As NIST identifies national trends and needs, it can be a primary driver, functioning in a proactive – not just a reactive – mode. NIST's technical expertise, knowledge of industry, its relationships, and the information it gathers from interactions with others via conferences and its work directly with other federal agencies, industry, and researchers are all crucial in making these determinations.

Using a variety of approaches and processes, NIST works with these stakeholders to identify areas where standards or guidelines are needed, evaluate proposals, and develop standards or other publications. As a well-respected and trusted technical authority in this field, NIST must balance these needs to ensure that its standards and guidelines are technically sound and have the confidence of the community. Retaining that respect and authority requires that NIST must be – and must be perceived as – a trustworthy steward of the public's interest and a leader in driving and identifying advances in cryptography.

NIST informs and involves stakeholders through:

- participation in SDO activities,
- regular interactions in professional forums, open solicitations for input,
- cryptographic competitions,
- early announcement of its intention to work in a specific area,
- extending invitations to external subject matter experts to work as NIST guest researchers,
- presentations and discussions at conferences and standards meetings,
- publication of draft documents for public review and comment, and
- providing feedback on how NIST has addressed comments.

NIST also seeks input by hosting and funding external experts.

NIST prioritizes its participation in meetings, conferences, SDOs and industry groups based on the expected impact of NIST's involvement. In addition, NIST has resource limits that affect the number of guest researchers and visiting scholars that can be accommodated. 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.

Federal Stakeholders

NIST works in multiple ways with federal stakeholders, especially the agencies that are required to use FIPS and are encouraged to use NIST SPs for non-national security systems. Mechanisms for meeting the needs of these organizations include the full range of vehicles NIST uses with others: encouraging participation in NIST conferences and workshops, NIST's participation in events organized by others, solicitations for input as NIST sets its agenda and proposes cryptographic standards and guidelines, and informal, one-on-one discussions. Some special collaborative arrangements, including memoranda of understanding (MOUs), are also used in working with these agencies.

Participation in the Federal Government's Chief Information Officer (CIO) Council and its committees offers another way for NIST to ensure that it has direct links with the community of leaders in the U.S. Government who are most interested in or affected by NIST's cryptographic standards and guidelines.

NIST sponsors the Federal Computer Security Managers Forum, an informal group that promotes information sharing among federal agencies regarding information system security. The forum hosts the Federal Agency Security Practices website, maintains an extensive e-mail list, and holds bi-monthly meetings to discuss current issues and items of interest to those responsible for protecting non-national security systems. The forum provides an opportunity for managers of federal security programs to exchange information system security materials and knowledge for use in other programs in a timely manner, build upon the experiences of other programs, and reduce possible duplication of effort. NIST uses the forum to engage federal agencies on cryptographic issues, including standards and guidelines.

From time-to-time, NIST is called upon by the Executive Office of the President to develop standards or guidelines related to cryptography for the protection of federal information systems. The Office of Management and Budget (OMB) is a primary stakeholder in its capacity of providing directions to agencies about their planning for and use of information technology resources, including the protection of non-national security federal information systems.

NIST brings its cryptographic expertise to bear on priority national issues when directed by Congress, the President, or OMB and it also assists individual agencies that have specific needs. Recent examples include secure electronic voting; protecting the electric power "smart grid;" and health information technology initiatives that must ensure the protection of personal and proprietary business data. This work may be accomplished through interagency agreements, other formal measures, or by informal consultation and collaboration. NIST dedicates resources

to these kinds of assistance efforts when they are directed by Congress, the President or OMB, when they are compatible with its mission, and where NIST has special expertise.

Multiple federal agencies contribute to NIST's cryptography efforts in research and in developing standards and guidelines. Consultation with several of those organizations – the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, the Government Accountability Office, and the Secretary of Homeland Security– is mandated by the Federal Information Security Management Act (FISMA) in order to avoid unnecessary and costly duplication of effort and to assure that NIST's standards and guidelines are complementary with those employed for the protection of national security systems and information contained in these systems.

Beyond this statutory requirement calling for NIST to consult with other agencies, the NSA, in particular, has significant expertise in cryptography. Their cooperation with NIST is governed by an MOU between the two agencies and technical staff meet monthly to discuss ongoing collaborative work and future priorities.

As part of other agencies' collaboration with NIST, their staff may assist in the development of new standards and guidelines. This may take the form of coauthoring publications with NIST staff, providing comments on draft documents, or submitting cryptographic algorithms for consideration by NIST. All significant contributions will be acknowledged appropriately. In accordance with NIST's authorship policy, NIST will identify the names of any authors of standards or guidelines. If a NIST standard or guideline contains an algorithm that was designed by another agency's employees, NIST will acknowledge that agency as the designer, even though NIST may not be able to list specific individuals[2]. As is the case with private sector organizations, NIST will consider and acknowledge other agencies' comments, whether they are provided during the formal public comment period or other stages of development. Comments from federal agencies received during the public comment period will be posted and adjudicated in the same way as those submitted by the public.

Another venue where NIST Interacts with NSA about cryptography is the Committee on National Security Systems (CNSS), where NIST is an observer. The CNSS is chaired by the Department of Defense, while the NSA staffs the CNSS Secretariat. The CNSS mission is to set national-level Information Assurance policies, directives, instructions, operational procedures,

[2] 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.

guidance and advisories for United States Government departments and agencies for the security of National Security Systems. NIST reviews and comments on drafts of proposed CNSS documents, including Policies, Directives, Instructions and Standards. The CNSS policy CNSSP-15 specifies the use of NIST standardized cryptographic algorithms for the protection of national security information.

Collaboration with these agencies helps NIST to identify, prioritize, and conduct work in cryptography. NIST also understands that having its own independent cryptographic expertise is essential in order to carry out the its statutory responsibility to develop strong cryptographic standards and guidelines to protect non-national security federal information systems. Moreover, this capability is vital to NIST's development of standards and guidelines that promote economic development and protect sensitive personal and corporate information.

Voluntary Standards Developing Organizations

NIST recognizes the important role that voluntary SDOs play in the global adoption of strong cryptography for the agency's various stakeholders. NIST is committed to pursuing a global acceptance strategy for NIST's cryptographic standards, and active participation in SDOs helps to ensure that NIST cryptographic standards and guidelines are highly secure and interoperable with those of international partners.

Based on need, impact, and industry interest, NIST decides how to engage with specific SDOs, which existing voluntary standards it can adopt or adapt, which standards may be best developed by an SDO rather than by NIST, and which of NIST's standards and guidelines are brought to SDOs for adoption.

Following federal policy contained in OMB Circular A-119[3] directing all agencies to use voluntary consensus standards in lieu of government-unique standards "except where inconsistent with law or otherwise impractical," NIST is committed to making maximum use of standards produced by SDOs as the first option in addressing a need for cryptographic standards. The section of this document, "*Policies and Processes for the Life Cycle Management of Cryptographic Standards and Guidelines*," provides detail about how NIST implements this strategy.

When NIST decides to develop a standard of its own, it will give strong consideration to submitting that standard to an SDO for broader acceptance, use, alignment, and impact. In the

[3] Office of Management and Budget, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, OMB Circular A-119 Revised, February 10, 1998. http://www.whitehouse.gov/omb/circulars_a119#1

past, SDOs have adopted important 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 Internet Engineering Task Force's (IETF) Transport Layer Security (TLS) protocol.

When selecting priorities for working with SDOs or using standards produced by those organizations, a major consideration for NIST is the degree of active participation in the SDO from cryptographic researchers, industry, and others in the user community.

NIST staff participates in SDOs either through a NIST membership in an organization (e.g., X9, Inc.[4] working groups, INCITS[5] technical committees) or as individuals (e.g., IEEE SA[6] working groups and IETF working groups). NIST experts also participate in some international SDOs through U.S. National Body or Member State representation. ANSI[7] is the sole U.S. representative for two major non-treaty international standards organizations, the International Organization for Standardization (ISO) and – via the U.S. 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 United States.

Working with SDOs provides an important avenue for outreach to and feedback from multiple stakeholders. In many cases, NIST staff members are contributors, editors, or working-group chairs for proposed voluntary standards that use cryptography. NIST participates in the SDO standards process along with industry involved in the design, development, and implementation of cryptography. This interaction promotes the exchange of information and provides early feedback on the effects of NIST standards and the need for new or different standards.

It is important that the roles of the NIST staff working with SDOs are very clear to all involved. NIST has agency-wide guidelines governing participation in SDOs.[8] These guidelines make it clear that participation in SDOs can, and must, tie directly to NIST's mission and key goals. IT security clearly falls within that realm.

The Research Community

[4] X9, Inc., Financial Industry Standards
[5] InterNational Committee for Information Technology Standards
[6] IEEE (Institute of Electrical and Electronics Engineers)
[7] American National Standards Institute
[8] N. Rioux, E. Puskar and M.J. DiBernardo, *Guidelines for NIST Staff Participating in Documentary Standards Developing Organizations' Activities*, NISTIR 7854, May 2012. http://dx.doi.org/10.6028/NIST.IR.7854.

NIST is deeply involved in the cryptographic research community through: participating in research conferences; serving as program committee members; serving as 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; funds academic research; and provides services, such as the NIST Randomness Beacon,[9] for the research community. As a result, cryptographers around the world often know the NIST contact in their area of interest – beyond their availability through NIST web pages about their work. NIST encourages and informally receives valuable informal information, often based on independent cryptanalysis, from researchers. When NIST proposes new FIPS or SPs – or changes to those publications – it reaches out to and relies on input from this community, and others, as an important part of the process.

Cryptographic algorithm competitions are an especially powerful vehicle for working with the research community to fill particular standards-related needs. They allow NIST to standardize a state-of-the-art, widely accepted cryptographic primitive by involving the international cryptographic research community in an open competition to select an algorithm that NIST will standardize and promote. Competitions are only one of several approaches for establishing a cryptographic standard; sometimes the needed standard has already been developed by an SDO and been well-accepted by the community. Moreover, competitions are very time- and resource-intensive. However, they can bring significant benefits when properly used. The section of this document, "*Policies and Processes for the Life Cycle Management of Cryptographic Standards and Guidelines*," provides details about how NIST approaches these competitions.

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

Public Notice and Review of Proposed and Final Standards and Guidelines

NIST strives to be as open and transparent as possible in its cryptographic standards and guidelines activities. That includes involving stakeholders from the time that NIST identifies an area of interest through the full life cycle of managing a standard or guideline. Public notice and review of proposed and final standards and guidelines is a key element. Basic features are noted below; details are described in the "*Policies and Processes for the Life Cycle Management of Cryptographic Standards and Guidelines*" section of this document.

NIST provides public notice of its most significant activities in cryptography, including:

- plans for cryptographic standards and guidelines, including seeking information from the public about available standards and guidelines or ongoing development work;
- invitations for public participation in NIST-sponsored workshops and conferences that discuss and advance topics in cryptography and its standardization;
- participation by NIST staff in workshops and conferences sponsored by other organizations on cryptography and standardization;
- announcements of draft cryptographic standards and guidelines for public review and comment; and
- announcements of NIST's responses to comments and posting of final publications.

All announcements are posted on the CSD website (http://csrc.nist.gov). Requests for comments on proposed FIPS, as well as announcements of the final FIPS, are published in the *Federal Register*[10]. When NIST is aware of SDOs working on related standards, NIST will reach out to relevant working groups to inform them of these announcements. In addition, press releases usually accompany significant announcements, and NIST Information Technology Laboratory (ITL) Security Bulletins provide information about the use of cryptographic standards and guidelines[11]. In some cases, NIST maintains a public email forum for ongoing open discussion of subjects relevant to cryptographic standards or research activities.

The primary public comment and feedback mechanism for NIST cryptographic standards and guidelines is the posting of drafts and requests for comment on the CSD website. Comment periods depend on the size and complexity of the drafts, as well as prior history of public exposure and commentary, but typically run from 30 to 90 days.

[10] http://www.federalregister.gov/

[11] http://csrc.nist.gov/publications/PubsITLSB.html

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.

NIST will track, post, and publicly respond to ***all*** comments received as a result of a request for comment on a draft FIPS or draft guideline, in compliance with applicable law. Comments received on draft FIPS, and their dispositions, are summarized in the *Federal Register* notice announcing the approval of a new or revised standard. All commenters are encouraged to use the public comment process to ensure that their comments are received and given due consideration. NIST will provide rationale for all substantive changes to draft documents, either as a response to a public comment or in a separate description and justification for the change.

For standards developed within consensus-based SDOs, feedback is generated and received in accordance with the policies and procedures of the respective SDOs. In these cases, in keeping with its own principles, NIST takes into account the transparency and openness of the environment in which those standards are developed before adopting or recommending a standard.

The value of NIST's processes for cryptographic standards and guidelines depends upon the active involvement of subject matter experts from the cryptographic community, as well as those organizations that use and depend on these standards and guidelines. NIST encourages all stakeholders to provide input throughout the process from start to finish – including but not limited to reviewing and commenting on drafts when they are posted for public comment.

Policies and Processes for the Life Cycle Management of Cryptographic Standards and Guidelines

NIST has policies and processes for the life cycle management of cryptographic standards and guidelines. These cover the initial identification and selection of areas to be addressed through development, solicitation and response to comments and recommendations, submission of standards for consideration by SDOs, and regular maintenance and review, including updating and withdrawing the approval of a standard or guideline. General approaches are described in the previous sections; process details are described below.

1. ***Triggers: Identify and Evaluate the Need***

   NIST considers a variety of factors in initially identifying the need for a cryptographic standard or guideline. Major considerations include:

   - *Is there a legal or administrative directive or guidance?* NIST has statutory requirements and high-level Executive Branch directives to undertake work in a particular area. These include statutory mandates (e.g., FISMA), Presidential Directives (e.g., Homeland Security Presidential Directive 12 (HSPD-12)), and OMB guidance (e.g., M-04-04).
   - *Did an environmental or technological development trigger a particular interest?* As processing speeds and memory get faster and cheaper, new advances in cryptography demand that NIST constantly monitor the strength and effectiveness of the algorithms in its standards and guidelines. Attacks and other security breaches can be triggering events. Research that shows vulnerabilities of a widely used cryptographic standard can be a motivation. NIST may hold workshops to assess the need, to discuss cryptographic research or proposed algorithms, or as part of a cryptographic competition, for example.
   - *Is it a compelling area for NIST's engagement?* Work on a new standard or guideline should be useful, first and foremost, to the Federal Government's ability to carry out its non-national security functions and to promote economic development. The work that is contemplated should have broad applicability, rather than simply fill a niche need.
   - *Does it appear to be a matter that the communities of interest consider to be both important and practical to address?* This could include identifying existing methods that are used to solve similar challenges within those communities.

2. ***Announce Intent to Work on a Standards or Guidelines Project***

   Once NIST identifies a need for a standard or guideline in a particular area and decides to work on a project, it will:

   - Publicly announce the need and its planned work on a project via the CSD website and other mechanisms. The announcement will provide the problem statement, a review of

possible approaches for producing a standard or guideline, and a rough development schedule.

- Solicit input though the website, presentations, newsletters, and workshops, and/or an open solicitation for comments.
- Issue formal requests for comments or information, as needed.

3. Consider Requirements and Solutions

To ensure that NIST has broad and in-depth knowledge of the challenge, requirements to be addressed, and potential solutions – including work by others – early in the process, NIST will:

- Identify the requirements and goals of the proposed standard or guideline project, for example, determine the desirable security properties and the evaluation criteria for assessing potential solutions.
- Investigate the literature and what solutions are incorporated into products and standards.
- Determine what kind of analysis has been done on various options and the most appropriate additional analysis to undertake. This work would include an analysis into the design of the cryptographic algorithm or scheme, including any constants used in the specification.
- Pursue security proofs for proposed cryptographic algorithms or schemes. While not a prerequisite for consideration, security proofs are useful tools for analyzing and vetting cryptographic algorithms being evaluated for inclusion in NIST standards and guidelines. The proofs are usually conducted based on assumptions about the basic components of the scheme using a specific threat model; the correctness of the proof and the applicability of the threat model must be evaluated alongside the algorithm. NIST will pursue these proofs and encourage their development and analysis by the research community. In solicitations for proposed algorithms, NIST will ask for these proofs and, when available, include them in the public record when standards and guidelines are developed.

4. Define a Specific Plan and Process

NIST has several approaches it may use to meet needs for cryptographic standards or guidelines. These include adopting or adapting existing SDO-produced standards, encouraging and participating in the development of new standards by SDOs, or developing NIST standards – which, in some cases, may involve holding a competition. NIST will solicit input from stakeholders in determining the most appropriate approach for a particular standard or guideline. After making a decision, NIST will state and explain publicly the reason for this determination. Options include:

- ***Work with SDOs***

  From the time that NIST first identifies a specific standards-related need, the agency will explore relevant SDO-developed standards that are available or already in process as an alternative to developing its own standards. If there is an existing standard that has been developed via a vigorous and documented participative process, NIST may choose to adopt the standard in its entirety or to provide guidelines for its use rather than develop its own standard.

  If a needed standard does not already exist, NIST will consider the potential for encouraging SDOs – while involving industry, the user community, and cryptographic researchers – to begin the process of developing such a standard. One important consideration is the development time required. NIST may consider assigning its own staff to participate in one or more SDO standards development efforts if the work is of sufficient priority and could potentially match its needs. The resources required to provide this support also will be taken into account.

- ***Develop a New Standard or Guideline***

  When NIST identifies a requirement for a standard and determines that no suitable standard already exists, NIST experts in cryptography may begin development of a new standard or guideline working in collaboration with experts in academia, industry and government. The development team is responsible for ensuring that NIST's principles and processes described in this document are followed throughout the development process. Transparency and collaboration are accomplished through formal public review processes and interaction with experts at public workshops and industry meetings. For the development of new cryptographic algorithms, NIST may invite contributions from the public. If the work has broad applicability, NIST will consider contributing that work to an SDO, bringing about broader acceptance, use, and impact.

- ***Hold a Competition***

  If NIST decides to pursue the development of a standard or guideline, it may use an open competition. When a competition is used, interested parties will have an opportunity to participate in the competition by reviewing core requirements and evaluation criteria, publishing research papers, submitting comments, and attending public workshops. Researchers worldwide contribute candidate designs and papers on the theory, cryptanalysis and performance of the candidates. 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 comments on NIST's proposed criteria. A subsequent *Federal Register* notice states the submission requirements, schedule and selection criteria. A candidate conference is held, usually collocated 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 includes 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.

NIST will consider the use of open competitions to establish cryptographic standards particularly when no consensus exists yet around the best algorithmic approach. Competitions work best when a proposed algorithm or scheme requires a great deal of new cryptanalysis, as these competitions can focus the attention of cryptographers around the world. Decisions to use competitions will be made while recognizing and considering that these competitions are lengthy and resource intensive.

5. Develop NIST Federal Information Processing Standard (FIPS) or Special Publication (SP) Guideline

If NIST concludes that it will produce a FIPS or SP, a multi-step process is used. NIST will:

- Announce its intent to develop a FIPS or SP via multiple mechanisms, including the NIST website, newsletters, public presentations, and direct notifications to relevant SDOs and communities of interest.
- As part of this announcement, seek information about existing standards, standards in development, guidelines, or other information that could inform and assist NIST in this effort.
- Request information on potentially pertinent patents (in initial solicitations for information as well as in its publication of draft standards). This includes disclosure, where possible, of issued U.S. patents, pending U.S. patent applications, and corresponding foreign patents and applications. (Note: In considering an algorithm that is or may be subject to patent protection, NIST may seek assurances from the patent holder that royalty-free or royalty-bearing licenses will be made available on a Reasonable and Non-Discriminatory (RAND) basis, and may also seek assurances that such RAND licenses will be royalty-free.
- Consider the option of using, adapting or profiling an existing standard or guideline, rather than producing an entirely new standard or guideline.

- Develop a draft FIPS or SP – which may be entirely new or based on an existing standard or specification – and post that draft for public comment via a *Federal Register* notice for a FIPS; also, NIST employs multiple communication channels to announce the draft standard. Time allotted for public comments is:
    - Minimum of 90 days for new FIPS
    - Minimum of 30 days for SPs and small revisions to existing FIPS

  Similar mechanisms are used for announcing and accepting comments on a draft SP, except that the *Federal Register* process will not be used.
- Release any significant analyses and evaluations of algorithms or schemes that have been made available to NIST, in accordance with applicable law.
- Specifications of new algorithms or schemes will include design rationale, including a description of the provenance of any constants used within the specification.
- Consider and post comments and NIST's disposition of those comments.
    - NIST will strongly encourage reviewers to submit written comments to ensure that these comments are properly captured, considered, and show traceability. All public comments on cryptographic standards and guidelines will be made public, in compliance with applicable law.
    - NIST will provide rationale for all substantive changes to draft documents, either as a response to a public comment or in a separate description and justification for the change.
- Decide whether to finalize the FIPS or SP, or revise it and seek another round of comments.
    - If there are no substantial changes, NIST will proceed to finalize the publication.
    - Where there are significant dissenting comments, NIST will determine whether all views have been given full consideration and whether an additional comment period would provide additional information, and proceed accordingly.
- Finalize and approve the document, including an internal NIST editorial review and NIST management review and approval. Guidelines are reviewed by the NIST ITL Director. For FIPS (standards), the NIST Director approves the publication prior to submission to the Secretary of Commerce for final approval and promulgation.
- Announce the final FIPS or SP via the CSD website and other communication channels. For FIPS, NIST will also publish a *Federal Regis*ter notice.

6. Consider Submitting Standards and Guidelines for Adoption by SDOs

Reflecting NIST's recognition of the value of having cryptographic standards and guidelines adopted by SDOs:

- All FIPS and SP guidelines developed by NIST will be considered for submission to an SDO for their consideration.

- Because of the resources required to support a submission (e.g., editors), NIST will consider the input from stakeholders on potential submissions when determining priorities for submission.
- Priority will be given to: standards and guidelines that are being adopted by industry; submissions to SDOs with international scope; and standards versus guidelines.

7. Maintain Standards and Guidelines: Reviewing, Updating, and Withdrawal

All cryptographic standards and guidelines must be reviewed and maintained regularly because of rapid technological advances, the specific applications and assets for which these standards and guidelines are used, the threat environment, and the tolerance for risk by a particular sector or organization. NIST is committed to periodic review and maintenance of all cryptographic standards and guidelines. Maintenance can include updating or withdrawing the publication. When each standard or guideline is published, NIST identifies when the document will be subject to a review of its relevance and for possible updating. NIST uses the following approach:

- Review standards and guidelines regularly. The planned review period is identified when the document is initially finalized; FIPS are reviewed at least every five years or more frequently if issues arise. This may involve seeking public comment on the applicability and currency of the standard or guideline. Comments on proposed updates to or withdrawal of FIPS will be solicited using the *Federal Register*.
- Make review results public, including any public comments received.
- Renew, update or withdraw the standard or guideline. Renewal involves keeping the document unchanged. Update involves making revisions to the document (technical and otherwise). Withdrawal may be immediate, or it may be a phased withdrawal ("sunsetting"). Some technical content of a withdrawn standard or guideline can potentially be moved to another new or existing standard or guideline.

  An analysis of comments received on existing FIPS will be published in the *Federal Register* and the comments posted on the CSD website; comments received on existing SPs will be posted on the CSD website. NIST also will announce its decision on any maintenance effort (e.g., document update, withdrawal) that will take place.

NIST will use the processes and procedures described above to develop future cryptographic standards and guidelines. These are designed to provide broad opportunity to offer input on its cryptographic standards and guidelines, and to maximize openness and transparency. Please address any comments regarding these principles, processes and procedures — and NIST's use of them in developing cryptographic standards and guidelines — to Chief, NIST Computer Security Division at crypto@nist.gov. All comments and NIST's responses will be posted on the CSD website.