

NISTIR 7977

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

The Cryptographic Technology Group

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

1 Table of Contents

2 Note to Reviewers..... 2

3 Introduction and Overview 6

4 Principles..... 7

5 Publications for NIST’s Cryptographic Standards and Guidelines 9

6 Engaging the Cryptographic Community 12

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

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

9 Guidelines 20

10 **Note to Reviewers**

11

12 “It is of paramount importance that NIST’s process for developing cryptographic
13 standards is open and transparent and has the trust and support of the cryptographic
14 community. This includes improving the discipline required in carefully and openly
15 documenting such developments.”

16 *Report of the NIST Visiting Committee on Advanced Technology, July 2014*

17

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

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

30 ***Additions and clarifications of principles to guide and govern NIST’s work on cryptographic*** 31 ***standards and guidelines***

32 NIST is adding the following principles and steps:

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

43 NIST is clarifying principles and steps:

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

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

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

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

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

86 *Interactions with Standards Developing Organizations*

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

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

110 *Strengthening NIST's Cryptographic Capabilities*

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

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

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

125 ***Comments Requested on This Revised Draft***

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

- 128 • Do the expanded and revised principles state appropriate drivers and conditions for
129 NIST’s efforts related to cryptographic standards and guidelines?
- 130 • Do the revised processes for engaging the cryptographic community provide the
131 necessary inclusivity, transparency and balance to develop strong, trustworthy standards?
132 Are they worded clearly and appropriately? Are there other processes that NIST should
133 consider?
- 134 • Do these processes include appropriate mechanisms to ensure that proposed standards
135 and guidelines are reviewed thoroughly and that the views of interested parties are
136 provided to and considered by NIST? Are there other mechanisms NIST should consider?
- 137 • Are there other channels or mechanisms that NIST should consider in order to
138 communicate most effectively with its stakeholders?

139 **Introduction and Overview**

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

148
149 The Computer Security Division (CSD), a part of the NIST Information Technology Laboratory
150 (ITL), is charged with carrying out these responsibilities. Cryptographic standards and guidelines
151 for the protection of federal information systems have always been a key component of this
152 effort. They must be robust and have the confidence of the cryptographic community in order to
153 be widely adopted and effective at securing information systems worldwide.

154 To ensure these standards and guidelines provide high quality, cost-effective security
155 mechanisms, NIST works closely with a broad stakeholder community to identify areas of need
156 and develop standards and guidelines. That community has expanded in recent years and now is
157 truly global in nature, as is the interest in having a system in place that will appropriately protect
158 and ensure the security of digitized information. That community includes experts from
159 academia and government agencies, and from sectors and organizations that choose to adopt
160 NIST cryptographic standards and guidelines. NIST knows – and has been reminded by
161 stakeholders – that open and transparent processes are critical to developing the most secure and
162 trusted cryptographic standards possible. NIST strives to engage all of its stakeholders in these
163 processes, and has strengthened its efforts. This document sets forth the principles and processes
164 NIST will use for future cryptographic standards and guidelines and reflects substantial
165 stakeholder input.

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

176 **Principles**

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

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

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

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

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

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

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

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

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

233 **Publications for NIST’s Cryptographic Standards and Guidelines**

234 NIST uses several types of documents to publish and disseminate its cryptographic standards and
 235 guidelines. Three categories of NIST publications are commonly used: Federal Information
 236 Processing Standards, NIST Special Publications, and NIST Interagency Reports. Draft and final
 237 cryptographic standards and guidelines are posted by NIST on its Computer Security Resource
 238 Center web pages (<http://www.csrc.nist.gov>) and are freely available to everyone.

239 ***Federal Information Processing Standards (FIPS)***: By federal statute¹, FIPS publications are
 240 issued by NIST after approval by the Secretary of Commerce. They are used by NIST to publish
 241 standards for fundamental cryptographic primitives, such as block ciphers, digital signature
 242 algorithms, and hash functions.

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

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

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

¹ 15 U.S.C. 278g-3, as amended.

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

269 **Stakeholders for NIST’s Cryptographic Standards and** 270 **Guidelines**

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

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

286 The national security community within the U.S. Federal Government has also adopted a subset
287 of NIST’s cryptographic standards and guidelines through the Suite B program. The National
288 Security Agency (NSA) has approved the algorithms that comprise Suite B to protect classified
289 information up to the Secret level, with a class of algorithms with larger key sizes approved to
290 protect information at the Top Secret level. Because of the national security sector’s use of NIST
291 cryptographic standards and guidelines, that sector is also an important stakeholder.

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

299 **Engaging the Cryptographic Community**

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

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

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

316 NIST informs and involves stakeholders through:

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

326 NIST also seeks input by hosting and funding external experts.

327 NIST prioritizes its participation in meetings, conferences, SDOs and industry groups based on
 328 the expected impact of NIST’s involvement. In addition, NIST has resource limits that affect the
 329 number of guest researchers and visiting scholars that can be accommodated. Within these
 330 constraints, NIST strives to keep stakeholders informed by reaching out to the community, being
 331 accessible for discussions, listening to concerns, responding to questions, making important

332 activities public, participating actively in the cryptographic research community, and supporting
 333 voluntary standards development efforts.

334 ***Federal Stakeholders***

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

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

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

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

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

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

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

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

381 As part of other agencies’ collaboration with NIST, their staff may assist in the development of
382 new standards and guidelines. This may take the form of coauthoring publications with NIST
383 staff, providing comments on draft documents, or submitting cryptographic algorithms for
384 consideration by NIST. All significant contributions will be acknowledged appropriately. In
385 accordance with NIST’s authorship policy, NIST will identify the names of any authors of
386 standards or guidelines. If a NIST standard or guideline contains an algorithm that was designed
387 by another agency’s employees, NIST will acknowledge that agency as the designer, even
388 though NIST may not be able to list specific individuals². As is the case with private sector
389 organizations, NIST will consider and acknowledge other agencies’ comments, whether they are
390 provided during the formal public comment period or other stages of development. Comments
391 from federal agencies received during the public comment period will be posted and adjudicated
392 in the same way as those submitted by the public.

393 Another venue where NIST Interacts with NSA about cryptography is the Committee on
394 National Security Systems (CNSS), where NIST is an observer. The CNSS is chaired by the
395 Department of Defense, while the NSA staffs the CNSS Secretariat. The CNSS mission is to set
396 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.

397 guidance and advisories for United States Government departments and agencies for the security
 398 of National Security Systems. NIST reviews and comments on drafts of proposed CNSS
 399 documents, including Policies, Directives, Instructions and Standards. The CNSS policy CNSSP-
 400 15 specifies the use of NIST standardized cryptographic algorithms for the protection of national
 401 security information.

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

408 ***Voluntary Standards Developing Organizations***

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

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

418 Following federal policy contained in OMB Circular A-119³ directing all agencies to use
 419 voluntary consensus standards in lieu of government-unique standards “except where
 420 inconsistent with law or otherwise impractical,” NIST is committed to making maximum use of
 421 standards produced by SDOs as the first option in addressing a need for cryptographic standards.
 422 The section of this document, “*Policies and Processes for the Life Cycle Management of*
 423 *Cryptographic Standards and Guidelines*,” provides detail about how NIST implements this
 424 strategy.

425 When NIST decides to develop a standard of its own, it will give strong consideration to
 426 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

427 past, SDOs have adopted important NIST cryptographic standards as foundational building
428 blocks for security protocols. For example, the Advanced Encryption Standard (AES) block
429 cipher is included in ISO/IEC 18033-3:2010, is the preferred block cipher for IEEE 802.11 to
430 secure wireless networks, and is mandatory to implement in version 1.2 of the Internet
431 Engineering Task Force's (IETF) Transport Layer Security (TLS) protocol.

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

435 NIST staff participates in SDOs either through a NIST membership in an organization (e.g., X9,
436 Inc.⁴ working groups, INCITS⁵ technical committees) or as individuals (e.g., IEEE SA⁶ working
437 groups and IETF working groups). NIST experts also participate in some international SDOs
438 through U.S. National Body or Member State representation. ANSI⁷ is the sole U.S.
439 representative for two major non-treaty international standards organizations, the International
440 Organization for Standardization (ISO) and – via the U.S. National Committee (USNC) – the
441 International Electrotechnical Commission (IEC). For treaty-based international standards
442 bodies, such as the International Telecommunication Union (ITU), the Department of State
443 represents the United States.

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

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

454 *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>.

455 NIST is deeply involved in the cryptographic research community through: participating in
456 research conferences; serving as program committee members; serving as speakers and
457 reviewers for conferences and workshops; and writing papers on NIST research. NIST also
458 invites and hosts guest researchers, postdoctoral fellows and visiting scholars; funds academic
459 research; and provides services, such as the NIST Randomness Beacon,⁹ for the research
460 community. As a result, cryptographers around the world often know the NIST contact in their
461 area of interest – beyond their availability through NIST web pages about their work. NIST
462 encourages and informally receives valuable informal information, often based on independent
463 cryptanalysis, from researchers. When NIST proposes new FIPS or SPs – or changes to those
464 publications – it reaches out to and relies on input from this community, and others, as an
465 important part of the process.

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

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

476 **Public Notice and Review of Proposed and Final Standards and**
 477 **Guidelines**

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

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

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

494 All announcements are posted on the CSD website (<http://csrc.nist.gov>). Requests for comments
 495 on proposed FIPS, as well as announcements of the final FIPS, are published in the *Federal*
 496 *Register*¹⁰. When NIST is aware of SDOs working on related standards, NIST will reach out to
 497 relevant working groups to inform them of these announcements. In addition, press releases
 498 usually accompany significant announcements, and NIST Information Technology Laboratory
 499 (ITL) Security Bulletins provide information about the use of cryptographic standards and
 500 guidelines¹¹. In some cases, NIST maintains a public email forum for ongoing open discussion of
 501 subjects relevant to cryptographic standards or research activities.

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

¹⁰ <http://www.federalregister.gov/>

¹¹ <http://csrc.nist.gov/publications/PubsITLSB.html>

506 If the nature or extent of changes to a draft resulting from the comments is sufficiently extensive,
507 one or more additional cycles of public review may be conducted.

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

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

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

525 **Policies and Processes for the Life Cycle Management of** 526 **Cryptographic Standards and Guidelines**

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

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

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

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

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

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

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

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

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

565 **3. Consider Requirements and Solutions**

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

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

587 **4. Define a Specific Plan and Process**

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

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

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

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

620 • **Hold a Competition**
 621 If NIST decides to pursue the development of a standard or guideline, it may use an open
 622 competition. When a competition is used, interested parties will have an opportunity to
 623 participate in the competition by reviewing core requirements and evaluation criteria,
 624 publishing research papers, submitting comments, and attending public workshops.
 625 Researchers worldwide contribute candidate designs and papers on the theory,
 626 cryptanalysis and performance of the candidates. The winning submitters are recognized,
 627 but agree to relinquish claim to intellectual property rights for their design so that the
 628 winning candidate can be available for royalty-free use. NIST determines the algorithm
 629 submission requirements and selection criteria, organizes workshops, hosts a competition
 630 website and e-mail discussion forum, selects the winning algorithm (based on its own
 631 analysis and that of the public), and explains and documents the selection.

632 A typical competition starts with a public dialog on the need and requirements for a new
 633 algorithm, both on-line and through public workshop(s), as well as a *Federal Register*
 634 announcement inviting comments on NIST’s proposed criteria. A subsequent *Federal*
 635 *Register* notice states the submission requirements, schedule and selection criteria. A
 636 candidate conference is held, usually collocated with a major cryptographic research
 637 conference, for each “round” of the competition to review the candidates and research
 638 results (i.e., cryptanalysis, performance and proofs of properties) on the candidates.
 639 Following each round, NIST announces the candidates selected to continue to the next
 640 round, and provides a report that documents the rationale for the selections. This
 641 winnowing allows the community to focus its analytical efforts on the most promising
 642 candidates. The last round usually includes about five strong candidates. Following the
 643 final candidate conference, NIST selects the winner, writes a final report and formally
 644 proposes a standard for the algorithm through the normal FIPS process.

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

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

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

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

- 670 • Develop a draft FIPS or SP – which may be entirely new or based on an existing standard
671 or specification – and post that draft for public comment via a *Federal Register* notice for
672 a FIPS; also, NIST employs multiple communication channels to announce the draft
673 standard. Time allotted for public comments is:
 - 674 ○ Minimum of 90 days for new FIPS
 - 675 ○ Minimum of 30 days for SPs and small revisions to existing FIPS
 676 Similar mechanisms are used for announcing and accepting comments on a draft SP,
677 except that the *Federal Register* process will not be used.
- 678 • Release any significant analyses and evaluations of algorithms or schemes that have been
679 made available to NIST, in accordance with applicable law.
- 680 • Specifications of new algorithms or schemes will include design rationale, including a
681 description of the provenance of any constants used within the specification.
- 682 • Consider and post comments and NIST’s disposition of those comments.
 - 683 ○ NIST will strongly encourage reviewers to submit written comments to ensure
684 that these comments are properly captured, considered, and show traceability. All
685 public comments on cryptographic standards and guidelines will be made public,
686 in compliance with applicable law.
 - 687 ○ NIST will provide rationale for all substantive changes to draft documents, either
688 as a response to a public comment or in a separate description and justification for
689 the change.
- 690 • Decide whether to finalize the FIPS or SP, or revise it and seek another round of
691 comments.
 - 692 ○ If there are no substantial changes, NIST will proceed to finalize the publication.
 - 693 ○ Where there are significant dissenting comments, NIST will determine whether
694 all views have been given full consideration and whether an additional comment
695 period would provide additional information, and proceed accordingly.
- 696 • Finalize and approve the document, including an internal NIST editorial review and
697 NIST management review and approval. Guidelines are reviewed by the NIST ITL
698 Director. For FIPS (standards), the NIST Director approves the publication prior to
699 submission to the Secretary of Commerce for final approval and promulgation.
- 700 • Announce the final FIPS or SP via the CSD website and other communication channels.
701 For FIPS, NIST will also publish a *Federal Register* notice.

702 **6. Consider Submitting Standards and Guidelines for Adoption by SDOs**

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

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

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

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

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

- 721 • Review standards and guidelines regularly. The planned review period is identified
- 722 when the document is initially finalized; FIPS are reviewed at least every five years
- 723 or more frequently if issues arise. This may involve seeking public comment on the
- 724 applicability and currency of the standard or guideline. Comments on proposed
- 725 updates to or withdrawal of FIPS will be solicited using the *Federal Register*.
- 726 • Make review results public, including any public comments received.
- 727 • Renew, update or withdraw the standard or guideline. Renewal involves keeping the
- 728 document unchanged. Update involves making revisions to the document (technical
- 729 and otherwise). Withdrawal may be immediate, or it may be a phased withdrawal
- 730 (“sunsetting”). Some technical content of a withdrawn standard or guideline can
- 731 potentially be moved to another new or existing standard or guideline.
- 732 An analysis of comments received on existing FIPS will be published in the *Federal*
- 733 *Register* and the comments posted on the CSD website; comments received on
- 734 existing SPs will be posted on the CSD website. NIST also will announce its decision
- 735 on any maintenance effort (e.g., document update, withdrawal) that will take place.

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