Preliminary Draft

NIST Special Publication 800-XXX
Revision 1 (2PreD) (June 01, 2018)

Title

Subtitle

Warning Notice

This document incorporates comments from the work-in-progress draft. It is a relatively cohesive document and is considered stable, although there are gaps in the content and the overall document is incomplete. Some changes are expected. Organizations may consider experimenting with guidelines, with the understanding that they will identify gaps and challenges. NIST welcomes early informal feedback and comments, which will be adjudicated after the specified public comment period; a full public draft is expected to follow.

Original Release Date

I N F O R M A T I O N S E C U R I T Y

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

NIST Special Publication 800-XXX
Revision 1 (2PreD) (June 01, 2018)

Title

Subtitle

First Author
Second Author
Third Author
Fourth Author
Fifth Author
Sixth Author

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-xxx

I N F O R M A T I O N S E C U R I T Y

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

NIST Special Publication 800-XXX
Revision 1 (2PreD) (June 01, 2018)

Title

Subtitle

First Author
Office of XXXX, First Operating Unit

Second Author
Office of XXXX, Second Operating Unit

Third Author
Office of XXXX, Third Operating Unit, Washington, DC

Fourth Author
Fourth Services, Inc., Reston, Virginia

Fifth Author
Fifth Services, Inc., Reston, Virginia

Sixth Author
Sixth Services, Inc., Reston, Virginia

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-xxx

June 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology
Special Publication 800-XXX Revision 1 (2PreD)
Natl. Inst. Stand. Technol. SP 800-XXX Revision 1 (2PreD), (June 2018)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-xxx

[2018-10-05: Comment period extended]

Public comment period: *2018-11-01* through *2018-11-30*

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Email: piv_comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Foreword

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. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

Include a brief abstract of the document. This can be the same text that is used in the NIST-114 form in NIKE. Any acronyms should be spelled out on first use (e.g., "Personal Identity Verification (PIV)…"). Avoid including references in this abstract. Guidance for writing Abstracts:

- Rule of thumb: limit to 200 words or less;
- Address the following questions:
  - What **problem** was examined or what procedure was carried out?
  - What was the **objective** of the activity being documented?
  - What was the **scope** of the activity?
  - What were the **principal conclusions and recommendations**?
- Use complete sentences;
- Acronyms: spell out upon first occurrence;
- Avoid unnecessary contractions or abbreviations;
- Avoid using equations and tables; and
- Avoid using "this draft" in the Abstract, for it can be easily overlooked when the final version is published

Keywords

The following are keywords to be used by search engines and document catalogues.

conditioning functions; entropy source; health testing; min-entropy; noise source; predictors; random number generators

Acknowledgements

For guidance on acknowledgements, see NIST Directive G 5201.01, *Guidance for Authorship of Scholarly and Technical Publications*, https://inet.nist.gov/directives/guidance-authorship-scholarly-technical-publications: "Personal Acknowledgement: Formal acknowledgement in a technical publication shall be accorded to individuals who have made at least one contribution to the project. Such

contributions can be of any type not meeting the requirements for authorship. Examples include routine programming support, laboratory equipment set-up, useful discussions, or extensive copy-editing of the publication."

Supplemental Context

An optional section with links to supplemental content that is integral to the document (e.g., Data DOI, URL for GitHub site with supporting documentation/software; project page on CSRC.nist.gov or another NISTsite, etc.). Should not include links to other SPs, FIPS, NISTIRs, etc. — that info should be in a Reference section or footnotes.

Audience

This document is intended for…

Document Conventions

Definitions of terminology for expressing recommended options (i.e., guidance), mandatory requirements, permissible actions, or possibilities. These could alternatively be specified in the introduction (e.g., Section 1), prior to specifying the technical content.

For Draft and Final publications: Per Annex A of the ITL Patent Policy, the document must also define the terminology used to express recommended options (i.e., guidance) and mandatory requirements. Terminology for expressing permissible actions or possibilities should also be defined. These definitions should ideally precede the technical content — possibly in a Document Conventions section in the front matter (see previous page) or in a subsection of the Introduction (e.g., in Section 1).

Example language is included in Annex A of ITL's Patent Policy (https://www.nist.gov/itl/publications-0/itl-patent-policy-inclusion-patents-itl-publications#annexa) and in the FAQ (https://inet.nist.gov/itl/frequently-asked-questions-itl-patent-policy-inclusion-patents-itl-publications).

Compliance with NIST Standards and Guidelines

Presently appears in FISMA-related SP 800s.

Conformance Testing

Some earlier publications included a statement in the Authority section to reference associated conformance testing. Those statements should be placed in this separate section.

For example, see the final paragraph in the Authority section of SP 800-56C (https://csrc.nist.gov/publications/nistpubs/800-56C/SP-800-56C.pdf), which reads "Conformance testing for implementations…"

Note to Readers

For FINAL publication only. If the present document revises/supersedes another publication, consider adding a very brief list that highlights changes/updates in the current version.

Trademark Information

…

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

1. assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or
2. assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:
    i) under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
    ii) without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: patent_piv_comments@nist.gov.

Executive Summary

The Executive Summary is an OPTIONAL section. It appears as part of the front matter (prior to the Table of Contents) and uses the front matter's roman numeral pagination.

Special Publications often include an Executive Summary, although it's not required. It can be particularly useful to the reader if the entire publication is rather long and detailed. This should be placed immediately before the Table of Contents in the front matter (using the roman numeral pagination). For examples, see SP 800-162, SP 800-153, SP 800-146, and SP 800-124 Revision 1.

General rules of thumb for the Executive Summary:

- Intended audience: managerial/policy role; a person who might be unlikely to read the entire publication.
- Style: written using language appropriate for the target audience
- Length: 5 to 10 % of the length of the main report content.
- Format: Start with a summary of the main report; write in the same order of the main report, using short and concise paragraphs.
- Self-contained: Readable as a standalone document, separate from the main report (i.e., don't include cross-references to other parts of the main report, including references; define acronyms).

Table of Contents

List of Figures

List of Tables

1. Introduction

Text

\[Wherever a link is included, e.g., https://www.nist.gov or [FIPS 140-2], add a ScreenTip to the link for Section 508 (accessibility) compliance. Right-click the link and select “ScreenTip” in the pop-up window. Add a generic statement, e.g., “Article link”, “NIST report link”, “Web page link”, etc.]

1.1. Second-level Heading

1.1.1. Third-level Heading

1.1.1.1. Fourth-level Heading

1.2. Subsection Two

Table info

Table 1 — Caption for Table One

Column Header 1	Column Header 2
A	B
C	D

Admonitions (like [TIP]) are used for text in boxes.

1.3. Document ConventionsA

If this is included in Section 1, it can be included as any subsection number. This just happens to be 1.3 in this template.

If the document includes recommended options (i.e., guidance) or mandatory requirements, then the terminology for expressing them must be defined. Terminology for expressing permissible actions or possibilities should also be defined. This should ideally precede the technical content, possibly in an introductory subsection like this, or in the front matter (see “Document Conventions” in the preface). Also see the related note above, following the Call for Patent Claims.

1.4. Subsection Four

General Guidance for References and Footnotes:

TEXT TO BE FINALISED ONCE NUMERIC REFERENCES IMPLEMENTED

References: Authors can choose between using numeric ("[1]") and alphanumeric ("[SP 800-300]") references but should use one or the other.

Authors should only use AsciiDoc cross-references in the body of the text; Metanorma will automatically insert the appropriate numeric or alphanumeric codes, retrieved from the References entry with the same cross-reference.

Numeric references will start with [1] and proceed sequentially for each new reference. If beginning a sentence with a numeric reference, start the sentence with "Reference [xyz]" (which will be rendered as "Reference [n]").

Alphanumeric references can be useful when there are numerous references to other specifications, and having the document number as part of the reference provides useful context to the reader (so they don't have to constantly navigate to the references section to see what's being cited).

Instead of hyperlinking a reference to an external URL, references should be either linked or cross-referenced to the applicable reference in the References section/appendix. Include the correct URL or DOI in the reference. If it ever needs to be update, it can then be (easily!) updated in just one place in the document.

Footnotes[1] can be used but should be used to provide context to the footnoted text. If the footnote includes a link to a referenced source, provide a link or cross-reference to the reference in the References section/appendix

[1]Standard footnote.

2. Section Two Heading

Text.

Figure info:

Improve accessibility by adding Alt Text or each figure.

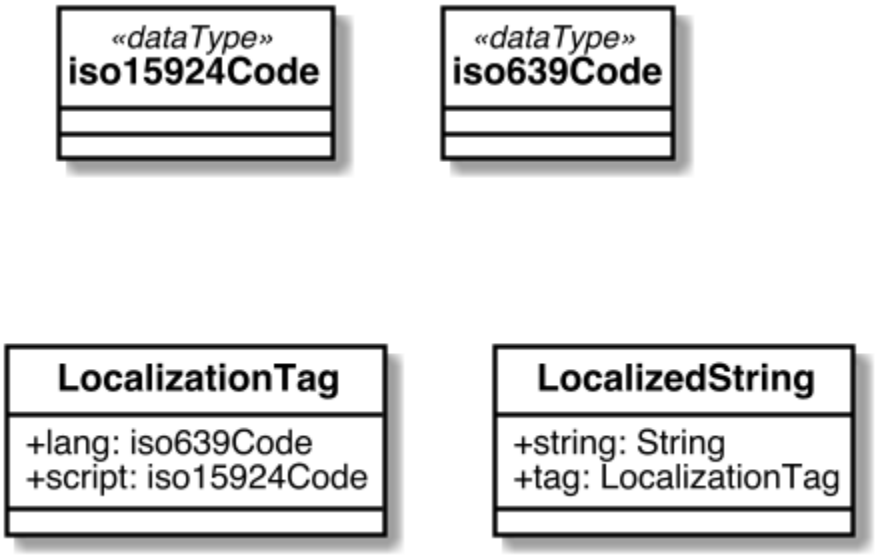

Figure 1 — Caption for Figure One.

Bibliography

Bhaumik R, Datta N, Dutta A, Mouha N, Nandi M (2017) The Iterated Random Function Problem. *23rd Annual International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2017*, (Springer, 12/07/2017), pp 667-697. https://doi.org/10.1007/978-3-319-70697-9_23 [Bhaumik_2017]

Souppaya MP, Regenscheid AR, Cooper DA, Cooley D, Bean C, Jenkins M, Boyle M (2018) *Security Considerations for Code Signing*. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01262018 [Boyle_2018]

Title 32 Code of Federal Regulations, Sec. 2002.4, *Definitions*. July 1, 2018 ed. https://www.govinfo.gov/app/details/CFR-2018-title32-vol6/CFR-2018-title32-vol6-sec2002-4 [CFR_2018]

E-Government Act of 2002, Pub. L. 107-347, 116 Stat 2899. https://www.govinfo.gov/app/details/PLAW-107publ347 [EGA_2002]

Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. https://www.govinfo.gov/app/details/FR-2013-02-19/2013-03915 [EO_13636]

National Institute of Standards and Technology (December 2002) *Security Requirements for Cryptographic Modules*, December 2002. https://doi.org/10.6028/NIST.FIPS.140-2.

Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283 [FISM_2014]

"Establishment of NIST Smart Grid Advisory Committee and Solicitation of Nominations for Members," 75 *Federal Register* 7 (January 12, 2010), pp 1595-1596. https://federalregister.gov/a/2010-344 [FR_7]

Alhebaishi N, Wang L, Jajodia S, Singhal A (2018) Modeling and Mitigating the Insider Threat of Remote Administrators in Clouds. *IFIP Annual Conference on Data and Applications Security and Privacy*, (Springer, 07/10/2018), pp 3-20. https://doi.org/10.1007/978-3-319-95729-6_1 [IFIP_2018]

International Organization for Standardization, International Electrotechnical Commission (June 2011) *Information technology — Security techniques — Information security risk management*, June 2011. ISO/IEC 27005:2011. URN urn:iso:std:iso-iec:27005:stage-95.99:ed-2. https://www.iso.org/standard/56742.html.

Kuhn R, Raunak M, Kacker RN (2017) It Doesn't Have to Be Like This: Cybersecurity Vulnerability Trends. *IT Professional* 19(6):66-70. https://doi.org/10.1109/MITP.2017.4241462 [MITP_2017]

National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018 [NIST CSF]

Paulsen C, Boyens J, Bartol N, Winkler K (April 2018) *Criticality analysis process model: prioritizing systems and components* (National Institute of Standards and Technology, Gaithersburg, MD), NIST NISTIRs (Interagency/Internal Reports) (IR) 8179, April 2018. https://doi.org/10.6028/NIST.IR.8179.

Office of Management and Budget (OMB), *E-Authentication Guidance for Federal Agencies*, OMB Memorandum 04-04, December 16, 2003. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2004/m04-04.pdf [OMB_2003]

Perlner RA , Liu Y-K (2018) Thermodynamic Analysis of Classical and Quantum Search Algorithms. *Quantum Information Processing*, (Delft, The Netherlands). https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=924493 [Perlner_2018]

D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk (May 2008) *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* RFC 5280, May 2008. IETF RFC 5280. DOI 10.17487/RFC5280. https://www.rfc-editor.org/info/rfc5280.

Dr. Ron S. Ross, Kelley L. Dempsey, Patrick Viscuso, Mark Riddle, Gary Guissanie (June 2018 (updated June 2018)) *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, June 2018 (updated June 2018). https://doi.org/10.6028/NIST.SP.800-171r1.

Scott W. Rose, Stephen Nightingale, Simson L. Garfinkel, Ramaswamy Chandramouli (September 2016) *Trustworthy Email*, September 2016. https://doi.org/10.6028/NIST.SP.800-177.

Jeffrey A. Cichonski, Joshua M. Franklin, Michael Bartock (December 2017) *Guide to LTE Security*, December 2017. https://doi.org/10.6028/NIST.SP.800-187.

U.S. Department of Homeland Security, U.S. Department of Commerce (2018) *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*. (U.S. Department of Commerce, Washington, DC). Available at https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf [US_2018]

National Institute of Standards and Technology, *Cybersecurity Framework* [Web site]. Available at https://www.nist.gov/cyberframework/ [Website_example]

Appendix A — Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

Acronym 1	Term 1
Acronym 2	Term 2

Appendix B — Glossary

For the purposes of this document, the following terms and definitions apply.

Term 1 Definition

Term 2 Definitin

Term 3 Definition