



NIST Special Publication 800
NIST SP 800-171Ar3

Assessing Security Requirements for Controlled Unclassified Information

Ron Ross
Victoria Pillitteri

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-171Ar3>

NIST Special Publication
NIST SP 800-171Ar3

Assessing Security Requirements for Controlled Unclassified Information

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-171Ar3>

May 2024



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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. Many NIST cybersecurity publications, other than the ones noted above, are available at <https://csrc.nist.gov/publications>.

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 [1]. 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 [2].

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.

NIST Technical Series Policies

[Copyright, Use, and Licensing Statements](#)

[NIST Technical Series Publication Identifier Syntax](#)

Publication History

Approved by the NIST Editorial Review Board on 2024-04-23

Supersedes NIST Special Publication 800-171A (June 2018) <https://doi.org/10.6028/NIST.SP.800-171A>

How to Cite this NIST Technical Series Publication:

Ross R, Pillitteri V (2024) Assessing Security Requirements for Controlled Unclassified Information and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171Ar3. <https://doi.org/10.6028/NIST.SP.800-171Ar3>

Author ORCID iDs

Ron Ross: 0000-0002-1099-9757

Victoria Pillitteri: 0000-0002-7446-7506

Submit Comments

800-171comments@list.nist.gov

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

Additional Information

Additional information about this publication is available at <https://csrc.nist.gov/pubs/sp/800/171/a/r3/final>, including related content, potential updates, and document history.

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

Abstract

The protection of Controlled Unclassified Information (CUI) is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully conduct its essential missions and functions. This publication provides organizations with assessment procedures and a methodology that can be used to conduct assessments of the security requirements in NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. The assessment procedures are flexible and can be customized to the needs of organizations and assessors. Assessments can be conducted as independent, third-party assessments or as government-sponsored assessments. The assessments can be applied with various degrees of rigor based on customer-defined depth and coverage attributes.

Keywords

assessment; assessment method; assessment object; assessment procedure; assurance; Controlled Unclassified Information; coverage; FISMA; NIST Special Publication 800-171; NIST Special Publication 800-53A; nonfederal organization; nonfederal system; security assessment; security requirement.

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. 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.

Audience

This publication serves a diverse group of individuals and organizations in the public and private sectors, including individuals with:

- System development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, system/security engineers, systems integrators)
- Acquisition or procurement responsibilities (e.g., contracting officers)
- System, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers)
- Security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts)

The above roles and responsibilities can be viewed from two perspectives:

- *Federal perspective*: The entity establishing and conveying security assessment requirements in contractual vehicles or other types of agreements
- *Nonfederal perspective*: The entity responding to and complying with the security assessment requirements set forth in contracts or agreements

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

1. Introduction.....1

1.1. Purpose and Applicability..... 1

1.2. Organization of This Publication 1

2. The Fundamentals.....3

2.1. Assessment Procedures 3

2.2. Assurance Cases 5

3. The Procedures7

3.1. Access Control..... 7

3.2. Awareness and Training 22

3.3. Audit and Accountability..... 25

3.4. Configuration Management..... 32

3.5. Identification and Authentication 42

3.6. Incident Response 49

3.7. Maintenance 54

3.8. Media Protection 57

3.9. Personnel Security 62

3.10. Physical Protection..... 64

3.11. Risk Assessment 69

3.12. Security Assessment and Monitoring 71

3.13. System and Communications Protection..... 75

3.14. System and Information Integrity 83

3.15. Planning..... 89

3.16. System and Services Acquisition 92

3.17. Supply Chain Risk Management..... 94

References.....99

Appendix A. Acronyms100

Appendix B. Glossary101

Appendix C. Security Requirement Assessment.....103

Appendix D. Organization-Defined Parameters107

Appendix E. Change Log112

List of Tables

Table 1. Security Requirement Families	3
Table 2. Summary of Assessment Preparation Phase.....	104
Table 3. Summary of Assessment Plan Development Phase.....	105
Table 4. Summary of Assessment Execution Phase.....	106
Table 5. Summary of Assessment Analysis, Documentation, and Reporting Phase	106
Table 6. Organization-Defined Parameters.....	107
Table 7. Change Log	113

Acknowledgments

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors whose constructive comments improved the overall quality, thoroughness, and usefulness of this publication. The authors also wish to thank the NIST technical editing and production staff – Jim Foti, Jeff Brewer, Eduardo Takamura, Isabel Van Wyk, Cristina Ritfeld, Derek Sappington, and Chris Enloe – for their outstanding support in preparing this document for publication.

Historical Contributions

The authors wish to acknowledge the following individuals for their historic contributions to this publication: Jon Boyens, Devin Casey, Ned Goren, Gary Guissanie, Jody Jacobs, Jeff Marron, Vicki Michetti, Mark Riddle, Mary Thomas, Gary Stoneburner, Patricia Toth, and Patrick Viscuso.