NIST Special Publication 800
NIST SP 800-60r2 iwd

Guide for Mapping Types of Information and Systems to Security Categories

Initial Working Draft

Joint Task Force

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-60r2.iwd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800
NIST SP 800-60r2 iwd

Guide for Mapping Types of Information and Systems to Security Categories

Initial Working Draft

Joint Task Force

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-60r2.iwd

January 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. 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.

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 YYYY-MM-DD [Will be added in final publication.]
Supersedes NIST Series XXX (Month Year) DOI [Will be added in final publication.]

How to Cite this NIST Technical Series Publication

Joint Task Force (2024) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-60r2 iwd. https://doi.org/10.6028/NIST.SP.800-60r2.iwd

Author ORCID iDs

Victoria Yan Pillitteri: 0000-0002-7446-7506
Naomi Lefkowitz: 0000-0003-3777-3106
Meghan Anderson: 0009-0004-2875-5672

Public Comment Period
January 31, 2024 – March 18, 2024

Submit Comments
sec-cert@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

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

Abstract

NIST Special Publication (SP) 800-60 facilities the application of appropriate levels of information security according to a range of levels of impact or consequence that may result from unauthorized disclosure, modification, or use of the information or systems. This publication provides a methodology to map types of information and systems to security categories (i.e., confidentiality, integrity, and availability) and impact levels (i.e., low, moderate, and high), a catalog of federal information types and recommended provisional impact levels.

Keywords

categorization; controlled unclassified information; cybersecurity; FISMA; information security; information taxonomy; information type; Risk Management Framework; RMF; security category; security categorization; system categorization.

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.

Supplemental Content

A proposed update to the information types taxonomy is available for review and download at the NIST SP 800-60 Initial Working Draft Publication Details page: https://csrc.nist.gov/pubs/sp/800/60/r2/iwd.

Note to Reviewers

NIST seeks to update and improve the guidance in Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*. Specifically, NIST seeks feedback on the current use, potential/proposed updates, and opportunities for ongoing improvement to SP 800-60.

NIST is proposing updates to the information types categorization methodology to better address privacy considerations during security categorization and align with updates in SP 800-37r2 (Revision 2), *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. Additionally, NIST intends to update the information types taxonomy and provisional impact levels (Volume 2) to ensure that they are consistent with current federal information types, including the NARA CUI registry, and allow for a more user-friendly and useable experience.

We welcome any general feedback related to mapping types of information and systems to security categories, as well as responses to the following:

- How does your organization use SP 800-60?
- If applicable, how does your organization use SP 800-60 to address PII?
    - Does your organization currently use SP 800-122 to help categorize PII?
- NIST intends to incorporate relevant guidance from SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, into the new draft revision of SP 800-60 and withdraw SP 800-122. What guidance (or topic areas) are critical to include in an SP 800-60 update?
    - What are other privacy considerations during security categorization?
    - Are there other important relationships between privacy and information types that should be covered? If so, what should be highlighted?
- What currently works well in SP 800-60?
- What are opportunities for improvement?
- Any other feedback on:
    - Updates to the security categorization methodology
    - Preliminary analysis and taxonomy for the information types catalog
    - Proposed next steps

Following the feedback received on this pre-call for comments, NIST plans to issue an initial public draft update to SP 800-60. The methodology will be issued as a document for comment, and the information types and provisional impact levels will be issued in a spreadsheet format for comment and then via the Cybersecurity and Privacy Reference Tool when finalized.

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:

a) 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

b) 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: sec-cert@nist.gov

Table of Contents

Acknowledgments

This publication was developed by the Joint Task Force Interagency Working Group. The group includes representatives from the civil, defense, and intelligence communities. NIST wishes to acknowledge and thank the senior leaders of the Departments of Commerce and Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency working group whose dedicated efforts contributed significantly to this publication.

Department of Defense

John Sherman, *Chief Information Officer (CIO)*

Leslie Beavers, *Principal Deputy CIO*

David McKeown, *Deputy CIO for Cybersecurity and Chief Information Security Officer*

Gurpreet Bhatia, *Principle Deputy CIO for Cybersecurity*

National Institute of Standards and Technology

James St. Pierre, *Acting Director, Information Technology Laboratory*

Kevin Stine, *Cybersecurity Advisor, Information Technology Laboratory*

Matthew Scholl, *Chief, Computer Security Division*

Victoria Yan Pillitteri, *Risk Management Framework Project Leader*

Office of the Director of National Intelligence

Dr. Adele Merritt, *Chief Information Officer*

Mike Castelli, *Acting Deputy CIO*

Kathryn Knerler, *Chief Information Security Officer*

Committee on National Security Systems

David McKeown, *Chair – Defense Community*

Katheryn Knerler, *Tri-Chair –Intelligence Community*

Christopher DeRusha, *Tri-Chair – Civil Agencies*

McKay Tolboe, *Subcommittee Tri-Chair – Defense Community*

Chris Johnson, *Subcommittee Tri-Chair – Intelligence Community*

Nicholas Polk, *Subcommittee Tri-Chair – Civil Agencies*

Joint Task Force Working Group

Victoria Yan Pillitteri NIST, JTF Leader	Ron Ross NIST	Naomi Lefkowitz NIST	Jon Boyens NIST
Meghan Anderson NIST	Derek Sappington NIST	Robert Byers NIST	Cristina Ritfeld NIST
Jeff Brewer NIST	Rebecca McWhite NIST	Eduardo Takamura NIST	Jeremy Licata NIST
Jeffrey Eyink DOD CIO	Robert Mawhinney DOD CIO	Mckay Tolboe DOD CIO	Chris Johnson Intelligence Community
Leo Yuwono Intelligence Community	Joseph Walker Intelligence Community	Larry Clark NARA ISOO	Tod Dabolt Department of Interior
Julie Snyder MITRE	Christina Sames MITRE	John Ferguson MITRE	Pam Miller MITRE
Randy Gabel MITRE	David Black MITRE	Karen Quigg MITRE	Katie Isaacson MITRE

1. Introduction

Identifying the information processed on a system is essential to the proper selection of controls. Regardless of sector, organizations understand the impacts of confidentiality, integrity, and availability on its information and systems. This publication provides a methodology to map types of information and systems to security categories, a catalog of federal information types, and recommended provisional impact levels.[1]

1.1. Purpose and Applicability

The revision of this section will include minor updates to the content included in [SP 800-60v1r1] and is intentionally left out of this review cycle.

1.2. Relationship to Other Documents

The revision of this section will include minor updates to the content included in [SP 800-60v1r1] and is intentionally left out of this review cycle.

1.3. Document Organization

This document is organized as follows:

- **Section 2** provides an overview of the value of the categorization process to agency missions, security and privacy programs, and overall information technology (IT) management and describes the publication's role in the system development life cycle, the certification and accreditation process, and the NIST Risk Management Framework (RMF).
- **Section 3** provides the security objectives and corresponding security impact levels identified in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* [FIPS 199].
- The **References** section offers a complete list of cited works.
  Note: The revision of this section will include updates to reflect the latest terms used and is intentionally left out of this review cycle.
- **Appendix A** is the Glossary.
  Note: The revision of this section will include updates to reflect the latest terms used and is intentionally left out of this review cycle.
- **Appendix B** provides an overview of the Information Types Taxonomy and Provisional Impact Levels.

[1] While this initial working draft does not include recommended provisional impact levels, it does provide an updated proposed information taxonomy of federal information types based on the Office of Management and Budget Federal Enterprise Architecture (FEA) Business Reference Model (BRM) version 3.1 and the National Archives and Records Administration (NARA) Controlled Unclassified Information (CUI) Registry Categories.

For a list of the proposed information types taxonomy in spreadsheet format, refer to the SP 800-60 Initial Working Draft Publication Details page.

This initial working draft only includes proposed updates for the information taxonomy for consideration; draft provisional impact levels are intentionally not included at this stage. When SP 800-60 is finalized, the information taxonomy and provisional impact levels will be published and maintained as an online dataset through the NIST Cybersecurity and Privacy Reference Tool.

2. The Fundamentals

Identifying the information processed on a system is essential to the proper selection of controls and ensuring the confidentiality, integrity, and availability of the system and its information. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 has been developed to help Federal Government agencies categorize information and systems.

2.1. Role of Information Types and Security Categorization in the NIST Risk Management Framework (RMF)

- This document relies on tasks and outcomes from Prepare – System Level Step and provides further guidance for Task C-2 of the Categorize step.
- This section will include an overview of how security categorization provides input into all subsequent steps of the RMF.

2.2. Security Categories and Objectives

2.2.1. Security Categories

- This section will include an overview of Federal Information Processing Standard (FIPS) 199 [FIPS 199].

2.2.2. Security Objectives and Types of Potential Losses

- This section will include the definition of security objectives (confidentiality, integrity, availability), definition from the Federal Information Security Modernization Act (FISMA) 2002 [44 U.S.C., Sec. 3542], and the corresponding [FIPS 199] definition.

2.3. Security Categorization and Privacy

2.3.1. Relationship Between Security Risk and Privacy Risk

- While security and privacy are independent and separate disciplines, their objectives can overlap.
    - Security programs are responsible for protecting information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized system activity or behavior) to provide confidentiality, integrity, and availability.

- Privacy programs are responsible for managing the risks to individuals associated with data processing throughout the information life cycle[2] and ensuring compliance with applicable privacy requirements.
- Although privacy risks can also arise by means unrelated to security incidents, this publication is focused on the overlap — namely, how the impact of security-related privacy events (i.e., potential problems that individuals could experience due to a loss of confidentiality, integrity, or availability) should be considered in security categorizations.

- Role of security objectives in protecting privacy
  - Security is one of the Fair Information Practice Principles (FIPPs) for privacy defined by OMB.
  - Although security cannot fully address privacy risk, it supports other FIPPs.
- Organizations determine how security and privacy work together to meet their specific needs in context.
- It is essential for organizations to take a coordinated approach to identifying and managing security and privacy risks.

2.3.2. Privacy and Information Types

- Many types of information may have privacy impacts, depending on the nature of data processing, such as personal identity and authentication (e.g., Social Security Numbers, names, dates of birth, places of birth, parents' names) and customer services (e.g., contact information, demographic information, complaints about interactions with organizations).
- Some information types may directly introduce privacy risks. Others may not introduce privacy risks until combined with other information types or only under specific data processing conditions.
- An information type may be considered personally identifiable information (PII) in some data processing environments and not in others.
- These characteristics make it challenging to specify a list of information types that are "always" a privacy-related information type or PII.
- Even when an information type meets the OMB A-130 definition of PII,[3] the context of its use can alter the impact level.
  - For example, an organization may have three lists that contain the same PII data fields (e.g., name, address, phone number). The potential impacts to the affected

[2] The information life cycle includes the creation, collection, use, processing, dissemination, storage, maintenance, disclosure, or disposal (collectively referred to as "processing") of information.
[3] "Personally identifiable information" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

individuals and the organization are significantly different for each of the three lists.

1. People who subscribe to a general-interest newsletter produced by the organization
2. People who have filed for retirement benefits
3. Individuals who work undercover in law enforcement

2.3.3. Privacy Considerations During Security Categorization

- Based on the relationship between cybersecurity and privacy risk described in Sec. 2.3.1, categorization considers the adverse privacy impacts that relate to the loss of confidentiality, integrity, or availability.
- Security categorization is informed by the privacy requirements of the system, the types of information processed by the system, understanding how information is processed throughout operations and the information life cycle, and how the nature of processing may impact both organizations and individuals.
- Examples of some privacy considerations for each security objective (i.e., confidentiality, integrity, availability)

2.4. Impact Assessment

2.4.1. Impact Levels

- Overview of FIPS 199 impact levels (i.e., Low, Moderate, and High)
- Application of FIPS to the security category of information

2.4.2. Impact and the Information Life Cycle

- Determining security and privacy impacts to organizations and individuals requires not only identifying the information processed by a system but also how risk can change based on the impacts of processing during each stage of the information life cycle (or during “data processing”).
- Overview of the information life cycle, such as the stages through which information passes (i.e., creation or collection, processing, dissemination, use, storage, and disposition) to include destruction and deletion
- Example considerations for applying security impacts to the information life cycle

2.5. Role in the System Development Life Cycle (SDLC)

- When initial security categorization and subsequent updates to security categorization can occur during the SDLC

2.6. Uses of Categorization Information

- This section will provide potential uses for categorization information, such as:
    - Business impact analysis
    - Capital planning and investment control (CPIC) and enterprise architecture (EA)
    - System design
    - Contingency and disaster recovery planning
    - Information exchange agreements

3. Assignment of Impact Levels and Security Categorization

- This section provides a methodology for assigning security impact levels and security categorizations for information types and systems consistent with the organization's assigned mission and business functions based on FIPS 199.

3.1. Step 1: Identify Information Types

- This section will be updated to better align with the structure and presentation of the Steps and Tasks in the NIST RMF. It will identify the outcomes of each step/task, potential inputs, expected outputs, relationship to the RMF (i.e., steps/tasks), primary responsibilities, supporting roles, and additional discussions.
- Task 1: Identify information types that are input into, stored, processed, and/or output from the system.

3.2. Step 2: Determine Information Type Impact Level

- Task 1: Select Provisional Impact Level (if applicable)
- Task 2: Tailor Provisional Impact Level or assign Preliminary Impact Level
    - FIPS 199 Security Categorization Criteria
    - Common Factors for the Selection of Impact Levels (i.e., confidentiality, integrity, and availability)
- Task 3: Review Provisional Impact Levels and adjust/finalize Information Type Impact Levels

3.3. Step 3: Assign System Security Category

- This section will include guidelines for system categorization and considerations such as aggregation, critical system functionality, extenuating circumstances, and other system factors (e.g., integrity of public information, catastrophic loss of system availability, large supporting and interconnecting systems, critical infrastructure, and privacy considerations)
- Task 1: Review considerations for system categorization
- Task 2: Assign overall system impact

3.4. Step 4: Document the Security Categorization Process

- This section will include guidelines for documenting the security categorization process, including the relationship to SP 800-18 and applicability in governance, risk, and compliance (GRC) tools.

References

The revision of this section will include updates to reflect the latest references used and is intentionally left out of this review cycle.

Appendix A. Glossary

The revision of this section will include updates to reflect the latest terms used and is intentionally left out of this review cycle.

Appendix B. Information Types Taxonomy and Provisional Impact Levels

Review the proposed information types taxonomy, which is available for download at the NIST SP 800-60 Initial Working Draft Publication Details page.

> This initial working draft includes a proposed update for the information taxonomy based ONLY on the *Federal Enterprise Architecture (FEA) Business Reference Model version 3.1*, Appendix H. Business Reference Model Taxonomy with Definitions and the National Archives and Records Administration (NARA) Controlled Unclassified Information (CUI) Registry Categories.
>
> When SP 800-60 is finalized, the information taxonomy, provisional impact levels, and mapping to the existing information types and provisional impact levels in SP 800-60 Volume II (2008) will be published as an online dataset through the *NIST Cybersecurity and Privacy Reference Tool*.

B.1. Business Reference Model Taxonomy Background

Per the Business Reference Model (BRM) version 3.1 Taxonomy (May 15, 2013),[4] "the BRM taxonomy is structured as a three-layer hierarchy representing Executive Branch ***Mission Sectors***, ***Business Functions*** and ***Services***."

- **Mission Sector** — Identifies the 10 business areas of the Federal Government in the Common Approach to Enterprise Architecture
- **Business Function** — Describes what the Federal Government does at an aggregated level, leveraging the budget function classification codes provided in OMB Circular A-11
- **Service —** Further describes what the Federal Government does at a secondary or component level

B.2. NARA CUI Registry Background

Per the NARA CUI Registry,

> Federal agencies routinely generate, use, store, and share information that, while not meeting the threshold for classification as national security or atomic energy information, requires some level of protection from unauthorized access and release. Protection may be required for privacy, law enforcement, or other reasons pursuant to and consistent with law, regulation, and/or Government-wide policy. Historically, each agency developed its own practices for sensitive unclassified information, resulting in a patchwork of systems across the Executive

[4] The BRM Version 3.1 Taxonomy is available at: https://obamawhitehouse.archives.gov/omb/e-gov/fea

> branch in which similar information might be defined and labeled differently, or where dissimilar information might share a definition and/or label, depending on the agency which originally created the information.
>
> The Controlled Unclassified Information (CUI) program represents an unprecedented initiative to standardize practices across more than 100 separate departments and agencies; State, local, Tribal and, private sector entities; academia; and industry, to enable timely and consistent information sharing, and to increase transparency throughout the Federal government and with non-Federal stakeholders. Sharing CUI is authorized for any lawful government purpose, defined as any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement).

Per the CUI Program Blog,

> CUI should be safeguarded at no less than the Moderate Confidentiality Impact level. The CUI Program draws on *National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53)* to establish the standards to safeguard CUI on Federal information systems.
>
> *NIST SP 800-171* establishes the standards to safeguard CUI on non-Federal information systems, such as those owned by contractors, universities, research labs, state and tribal governments, and other partners that receive or use CUI under contracts or agreements with the executive branch. Additional policy guidance can be found in *32 CFR 2002.14 (g)*.

Appendix C. Change Log

The revision of this section will include updates to reflect the latest terms used and is intentionally left out of this review cycle