NIST Internal Report
NIST IR 8278r1

National Online Informative References (OLIR) Program

Overview, Benefits, and Use

Nicole Keller
Stephen Quinn
Karen Scarfone
Matthew C. Smith
Vincent Johnson

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8278r1

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

NIST Internal Report
NIST IR 8278r1

National Online Informative References (OLIR) Program

Overview, Benefits, and Use

Nicole Keller
Stephen Quinn
Computer Security Division
Information Technology Laboratory

Matthew C. Smith
Huntington Ingalls Industries

Karen Scarfone
Scarfone Cybersecurity

Vincent Johnson
Electrosoft Services, Inc.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8278r1

February 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.

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 2024-02-23
Supersedes NIST IR 8278 (November 2020) https://doi.org/10.6028/NIST.IR.8278

How to Cite this NIST Technical Series Publication
Keller N, Quinn S, Scarfone K, Smith M, Johnson V (2024) National Online Informative References (OLIR) Program: Overview, Benefits, and Use. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8278r1. https://doi.org/10.6028/NIST.IR.8278r1

Author ORCID iDs
Nicole Keller: 0000-0003-4761-6817
Stephen Quinn: 0000-0003-1436-684X
Karen Scarfone: 0000-0001-6334-9486
Matthew C. Smith: 0000-0003-1004-7171
Vincent Johnson: 0000-0002-7363-996X

Contact Information
olir@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8278/r1/final, including related content, potential updates, and document history.

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

Abstract

Information and communications technology (ICT) domains — such as cybersecurity, privacy, and Internet of Things (IoT) — have many requirements and recommendations made by national and international standards, guidelines, frameworks, and regulations. An Online Informative Reference (OLIR) provides a standardized expression of the relationships between concepts in such documents. OLIRs provide a consistent and authoritative way to specify these relationships that can be used by both humans and automated tools. The National OLIR Program is a NIST effort to encourage and facilitate the definition of OLIRs by subject matter experts and to provide a centralized location for displaying and comparing OLIRs. This report provides an overview of the National OLIR Program, explains the basics of OLIRs and the benefits they can provide, and shows how anyone can access and use OLIRs.

Keywords

concept crosswalk; Informative Reference; National OLIR Program; Online Informative References (OLIRs); set theory relationship mapping; supportive relationship mapping.

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.

Audience

People who might benefit most from this publication include cybersecurity subject matter experts, framework developers and consumers, cybersecurity professionals, auditors, and compliance specialists.

Acknowledgments

Thanks to all of those who contributed to or commented on this document, particularly Murugiah Souppaya from NIST.

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

List of Tables

List of Figures

1. Introduction

Information and communications technology (ICT) domains — such as cybersecurity, privacy, and the Internet of Things (IoT) — have many requirements and recommendations made by national and international standards, guidelines, frameworks, and regulations. Your organization determines which standard, guideline, framework, and regulation documents it *must* follow as well as what it *chooses* to follow. Each of these documents has a unique set of requirements and recommendations, and document creators typically organize and present their content in whatever prose format and structure they find suitable.

You and your colleagues need to identify all of the applicable requirements and recommendations across all of these documents and to make sense of them in aggregate. Here are some notional examples of understanding relationships between them:

- Implementing a new security control *X* would help satisfy particular requirements and recommendations from other documents.
- You need to update your remote access policy to include a requirement from document *A* that is more stringent than the requirements from other documents. That policy update should help satisfy the corresponding requirements from the other documents.
- Your organization needs to comply with a new standard, so you need to determine which of its requirements you already meet, which you do not meet, and which potentially conflict with other requirements.

Knowing these things involves identifying the relationships among the requirements and recommendations from the documents. Making these determinations is usually time-consuming and prone to error, especially when you are not an expert on the documents.

Some documents include concept crosswalks, which provide basic information about which items in one document may relate to items in another document. For example, the NIST Cybersecurity Framework [1] adopted the term *Informative References* for its concept crosswalks; each Informative Reference indicates one or more parts of another document where readers can find additional information on the topic. Within the context of this document (and the National OLIR Program), a *concept crosswalk* indicates that a relationship exists between two items without any additional characterization of that relationship.

In a general sense, a mapping indicates how items contained in one document relate to items contained in another document. However, within the context of the documents and the National OLIR Program, *a set theory relationship mapping* indicates the relationships between elements (items) from two documents by both qualifying the rationale for indicating the connection between elements *(semantic, syntactic, or functional*) and classifying the relationship utilizing set theory principles (*subset of, intersects with, equal, superset of, not related to*). Another form of mapping, a *supportive relationship mapping*, indicates how a supporting concept (an item) can or does help achieve a supported concept (another item). One of the following relationship types must be specified for each supportive relationship: *supports, is supported by, identical, equivalent, or contrary*.

An *Online Informative Reference (OLIR)* records the relationships between elements of two documents as a concept crosswalk (a *concept crosswalk OLIR*), a set theory relationship mapping (a *set theory relationship mapping OLIR*), or a supportive relationship mapping (a *supportive relationship mapping OLIR*) in accordance with the OLIR specification. OLIRs are consistent, authoritative, and standardized expressions of relationships that can be used by both humans and automated tools. Automated approaches are often necessary because of the ever-expanding pool of documents. Separating OLIRs from the documents themselves also facilitates updating the OLIRs as needed instead of having to wait until a document containing OLIRs is updated and re-released. Future NIST publications are likely to use OLIRs instead of documenting relationships in an ad hoc manner within the publications themselves.

Each OLIR is formatted according to a simple method defined by NIST Internal Report (IR) 8278A Revision 1, *National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers* [2], and is displayed in a centralized location — the OLIR Catalog. The OLIR Catalog is publicly accessible, so you can use it to access, view, and download OLIRs for various pairs of documents.

1.1. Purpose and Scope

The purpose of this document is to introduce the National OLIR Program, highlight the benefits of OLIRs, and explain what OLIRs are and how to use the OLIR Catalog.

After reading this document, any subject matter experts (SMEs) interested in creating content for the OLIR Catalog should also read NIST IR 8278A Revision 1 [2], which provides information on how to define OLIRs and submit them to the Program.

1.2. Document Structure

The remainder of this document is organized into the following sections:

- Section 2 provides an overview of OLIR and the OLIR Catalog.
- Section 3 describes common uses of the OLIR Catalog.
- The References section lists the references cited in this publication.
- Appendix A contains a list of the acronyms used throughout this document.
- Appendix B provides a glossary of terminology used throughout this document.
- Appendix C offers a brief change log for this revision of the document.

2. OLIR Overview

The National OLIR Program is a NIST effort to provide a single online location — the OLIR Catalog — for displaying and comparing OLIRs for ICT domain documents. The Program uses the terms *OLIR*, *Informative Reference,* and *Reference* interchangeably. The Program defines a simple format in NIST IR 8278Ar1 [2] for expressing OLIRs in a standardized and consistent manner.

As part of the Program, NIST experts are defining OLIRs for NIST documents, such as:

- *The NIST Cybersecurity Framework (CSF) 2.0* [1]
- *Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* (Privacy Framework) version 1.0 [3]
- NIST IR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [4]
- Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* [5]

The Program also shows third parties how to define OLIRs for a document that they created or for which they are an SME and a document that is already represented in the OLIR Catalog. Creators of OLIRs are known as *OLIR Developers*, or simply *Developers*. The National OLIR Program defines a formal process for Developers to submit OLIRs to NIST [2]. This process includes guidance for creating high-quality, more usable, better-documented OLIRs. It also defines a managed process for reviewing, updating, and maintaining OLIRs as the documents they are based on are revised and updated. NIST encourages document owners, software vendors, service providers, educators, and other parties to develop and submit OLIRs to the National OLIR Program.

The National OLIR Program offers several benefits to anyone working with cybersecurity, privacy, or other ICT domain documents. Benefits include the following:

- The OLIR Catalog is a single, easy-to-use repository where you can obtain information on many documents and analyze their relationships. OLIRs provide a much more cost-effective method for you and others to establish and verify the relationships among the documents you use.
- Standardizing how relationships are expressed makes them more consistent, clear, usable, repeatable, and organizable, and it provides a way for automation technologies to ingest and utilize them.
- The National OLIR Program authenticates the source of each OLIR and allows you to identify who provided each OLIR.
- The National OLIR Program helps facilitate the integration of NIST guidance, which is produced in support of United States Government (USG) legislative and administrative responsibilities.

Note that although using OLIRs can significantly improve understanding of documents within organizations, it does not demonstrate or certify that an organization complies with a document. It can, however, assist in that process.

2.1. Understanding Relationships

Every OLIR compares elements of two documents and characterizes their relationship. The first document, called the *Focal Document*, is used as the basis for the comparison. All Focal Documents are NIST publications. The second document is called the *Reference Document*. Note that a Focal Document or a Reference Document is not necessarily in a traditional document format (e.g., a formal publication in a PDF) but could be a product, service, training, or other content. A *Focal Document Element* or a *Reference Document Element* is a discrete section, sentence, phrase, or other identifiable piece of content from a document.

A ***concept relationship style*** is an explicitly defined convention for characterizing relationships for a use case. NIST IR 8477, *Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines* [7] defines several concept relationship styles and provides more information on using them. The three concept relationship styles supported by OLIR are as follows:

- A ***concept crosswalk*** indicates that a relationship exists between a Focal Document Element and a Reference Document Element without any additional characterization of that relationship. Mappers may also choose to create a crosswalk for exploratory or preparatory purposes as the initial draft of a mapping that will eventually follow a more detailed relationship style. Section 4.1 of NIST IR 8477 provides additional information.
- A ***set theory relationship mapping*** indicates the relationships between a Focal Document Element and a Reference Document Element by both qualifying the rationale for indicating the connection between elements (semantic, syntactic, or functional) and classifying the relationship utilizing set theory principles (subset of, intersects with, equal, superset of, not related to). Section 4.3 of NIST IR 8477 provides additional information.
- A ***supportive relationship mapping*** indicates how a *supporting concept* can or does help achieve a *supported concept*, with one of the concepts being a Focal Document Element and the other a Reference Document Element. One of the following relationship types must be specified for each relationship: supports, is supported by, identical, equivalent, or contrary. Relationship properties can also be specified for the "supports" and "is supported by" relationship types. Section 4.2 of NIST IR 8477 provides additional information.

2.2. Relationship Strength

The National OLIR Program provides a means for an OLIR Developer to subjectively quantify the strength of a relationship between elements. This metric can provide additional insight for the implied bond between elements asserted by the Developer. Figure 1 illustrates how a single

relationship type can encompass relationships of different strengths. For example, Case 1 shows a Focal Document Element (f) and a Reference Document Element (r) in a Subset relationship with much in common, while Case 2 shows a Subset relationship where the two elements have relatively little in common. The other pairs of cases each depict different strengths of the same relationship type.

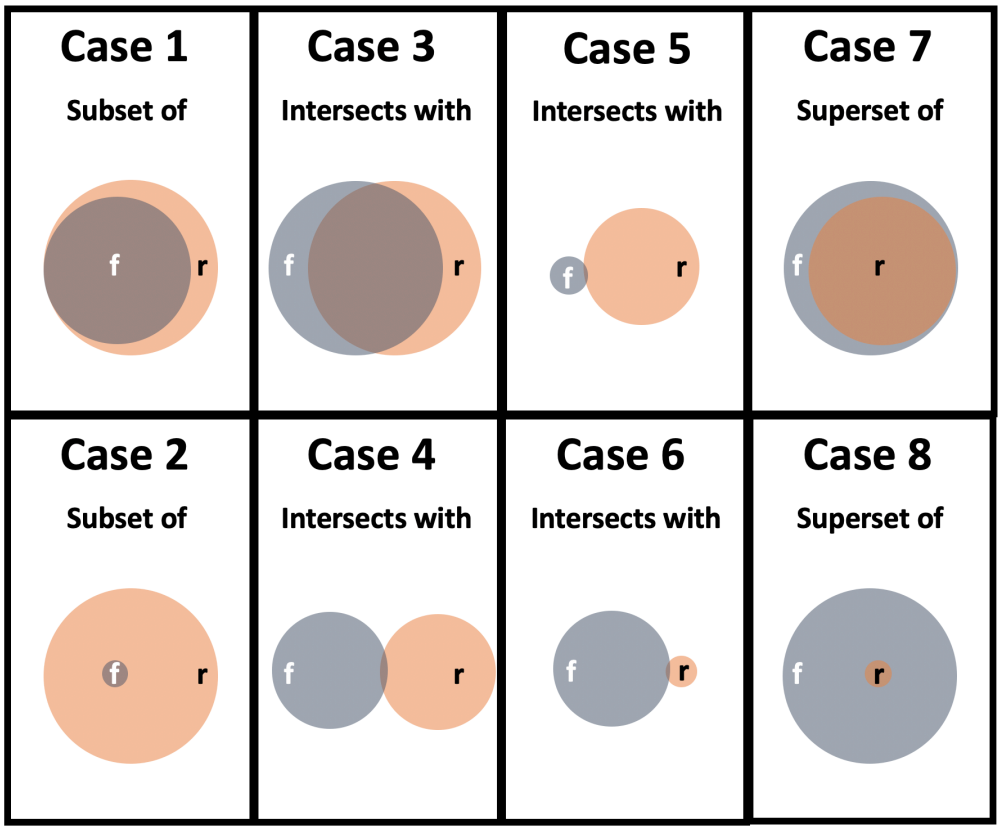


Fig. 1. Relative Strength of Relationships

The Program encourages OLIR Developers to include a characterization of the strength of comparable relationships but does not prescribe a methodology for doing so. Quantifying the strength of a relationship is optional, and its omission should not be interpreted as negative. It is intended for lateral comparisons, like the Cybersecurity Framework and the Privacy Framework, and not comparisons of documents at vastly different levels of abstraction, such as the Cybersecurity Framework and a research paper on a topic in quantum cryptography. The strength of non-lateral relationships is designated with "N/A."

2.3. Reference Data in the OLIR Catalog

The OLIR Catalog contains information on two types of relationships between Focal Documents and Reference Documents: OLIRs and Derived Relationship Mappings. These relationships are organized as *Reference Data* via the OLIR Catalog.

2.3.1. OLIRs

OLIRs have been vetted by NIST to ensure compliance with the NIST IR 8278A specification, submitted for a public comment period, and finalized. The National OLIR Program has two major source types for OLIRs:

1. **Owner:** These are produced by the owner of the Reference Document. For example, NIST is the owner of NIST SP 800-171 [6] and produced the OLIR for SP 800-171. Therefore, the designation of "owner" is granted to the SP 800-171 OLIR developed by NIST.
2. **Non-Owner:** These are produced by an SME other than the Reference Document owner.

Each OLIR is also categorized as either unilateral or bilateral, depending on which individuals or organizations created or validated it:

- **Unilateral:** NIST is not the owner of the Reference Document. The OLIR was created by a third party, and NIST has not validated the assertions made by the OLIR's Developer.
- **Bilateral:** NIST is the owner of the Reference Document. Either NIST has developed the OLIR (owner-produced OLIR), or a third party has developed the OLIR (non-owner-produced OLIR) and NIST has validated its assertions and reached agreement with the developer.

When multiple OLIRs are available for a particular Focal Document/Reference Document pair, consider the following:

- Generally, bilateral OLIRs should be favored over unilateral OLIRs.
- Generally, owner-produced OLIRs should be favored over non-owner-produced OLIRs.
- Generally, mapping OLIRs should be favored over crosswalk OLIRs.

If it is not clear which OLIR should be analyzed, focus on the quality and completeness of the OLIRs.

2.3.2. Derived Relationship Mappings (DRMs)

If OLIRs are not available for a particular Focal Document/Reference Document pair, you may be able to glean some of the mappings by using the OLIR Catalog's Cross-Reference Comparison Report tool. Derived relationship mappings (DRMs) are the result of using the OLIRs between two Reference Documents and a single Focal Document to make inferences about relationships between the two Reference Documents. Every OLIR submission uses standard identifiers for the Focal Document Elements, and these standard identifiers make it possible to associate Reference Document Elements with each other through their relationships to a common Focal Document Element. DRMs are dynamically generated when you use the Cross-Reference Comparison Report tool to search the OLIR Catalog. The results of the search are displayed to you, as Section 3.2 shows.

DRMs serve as the foundation for gap and comparative analysis. Figure 2 depicts how you could look for a relationship between Reference Document 1–Element A and Reference Document 2–Element B based on their individual relationships to Focal Document–Element E. DRMs do not indicate the relationships between the Reference Documents. Therefore, in reference to Fig. 2, if an organization implements Document 1–Element A, that does not necessarily mean it is also implementing Document 2–Element B. The two elements are *potentially* related. Even when the relationship is "equal," that does not mean the two elements are identical and does not imply that implementing one element means compliance with the other element.

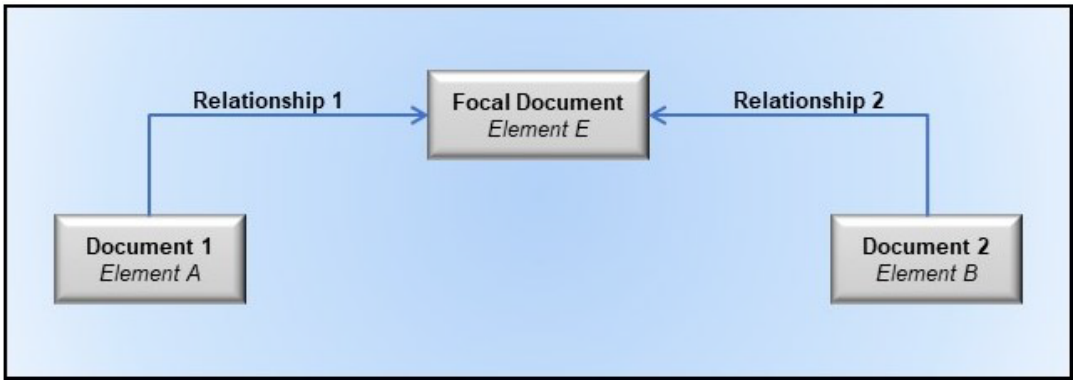


Fig. 2. Multiple Documents Related to a Focal Document

Another caveat regarding DRMs is that the elements being compared are often at different levels of detail (sometimes referred to as "different levels of abstraction"). For example, suppose you want to compare CSF Core Element PR.AC-01, "Identities and credentials for authorized users, services, and hardware are managed by the organization" [1], to NIST SP 800-53 Element IA-7, "Cryptographic Module Authentication," which is defined as "The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication" [5]. PR.AC-01 is at a higher level than IA-7, which specifies, in detail, one part of what PR.AC-01 encompasses. For some DRMs, the difference in the level of detail of the elements being compared may be vast.

Before the National OLIR Program, analyzing documents often meant you would have to conduct a manual comparison, perhaps by copying the contents of both documents into a spreadsheet for easier searching and sorting. You would then likely resort to using section headers as a starting point for the comparison because of a lack of consistent identifiers within the documents. For example, if you were comparing the Cybersecurity Framework with NIST SP 800-171 [6], you could review the "Asset Management (ID.AM) Category" of the Cybersecurity Framework Reference Document, then proceed to SP 800-171 and find a section where an element similar to the Cybersecurity Framework element might be documented. For this example, you might select Section 3.4, "Configuration Management," of SP 800-171 and read each of its basic and derived security requirements to identify relationships. You would repeat this laborious and error-prone process for all of the Categories and Subcategories within the Cybersecurity Framework and all of the basic and derived requirements of SP 800-171. Multiply this process by other people also finding the relationships, and two problems quickly emerge:

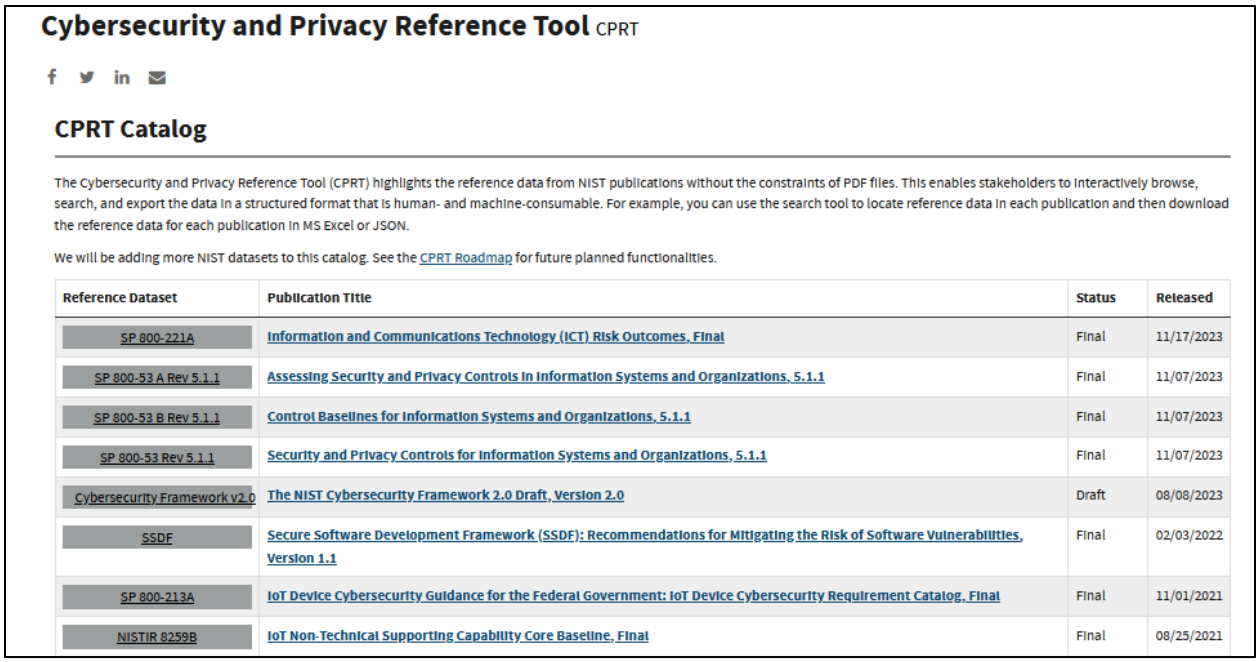
1) the different opinions of people result in inconsistent associations, and 2) an enormous amount of effort is duplicated. Streamlining this process is the main reason the OLIR DRM capability was created.

To save time, you can utilize DRMs. For example, you could leverage the OLIRs for Reference Document SP 800-171 to Focal Document SP 800-53 [5] and the OLIRs for Reference Document Cybersecurity Framework to Focal Document SP 800-53. SP 800-53 would serve as a transitive link for identifying commonality between the Cybersecurity Framework and SP 800-171. SP 800-171 Requirement 3.4.1 lists a relationship with SP 800-53 control CM-8. After you search the Cybersecurity Framework Core for mappings to CM-8, you see there is a relationship listed for Subcategories ID.AM-01, ID.AM-02, PR.PS-03, and DE.CM-09. You could then focus your comparative analysis on these elements.

Though the inferences that you may make while using DRMs are informative, **they are not considered verified nor authoritative**. DRMs can help you make better-informed decisions regarding risk management, compliance, control selection, and solution implementation activities, but they are only intended to aid you in conducting your own analysis, not to take the place of analysis.

2.4. NIST Cybersecurity and Privacy Reference Tool (CPRT)

The NIST Cybersecurity and Privacy Reference Tool (CPRT) project is a separate effort from OLIR, though it is a closely related and complementary resource. CPRT offers a consistent format for accessing reference data from selected NIST cybersecurity and privacy standards, guidelines, and frameworks in a unified data format, many of which are OLIR Focal Documents. CPRT provides a way to browse, view mappings, and download reference data from select NIST cybersecurity and privacy standards, guidelines, and Frameworks — all in standardized data formats (you can currently pick from Microsoft Excel [XLSX] or JavaScript Object Notation [JSON]). These tabular datasets will make it easier for users of NIST guidance to identify, locate, compare, and customize content without needing to review hundreds of pages of narrative within publications. The datasets are currently available for viewing within the CPRT Catalog, as Fig. 3 illustrates.



Cybersecurity and Privacy Reference Tool CPRT

CPRT Catalog

The Cybersecurity and Privacy Reference Tool (CPRT) highlights the reference data from NIST publications without the constraints of PDF files. This enables stakeholders to interactively browse, search, and export the data in a structured format that is human- and machine-consumable. For example, you can use the search tool to locate reference data in each publication and then download the reference data for each publication in MS Excel or JSON.

We will be adding more NIST datasets to this catalog. See the CPRT Roadmap for future planned functionalities.

Reference Dataset	Publication Title	Status	Released
SP 800-221A	Information and Communications Technology (ICT) Risk Outcomes, Final	Final	11/17/2023
SP 800-53 A Rev 5.1.1	Assessing Security and Privacy Controls in Information Systems and Organizations, 5.1.1	Final	11/07/2023
SP 800-53 B Rev 5.1.1	Control Baselines for Information Systems and Organizations, 5.1.1	Final	11/07/2023
SP 800-53 Rev 5.1.1	Security and Privacy Controls for Information Systems and Organizations, 5.1.1	Final	11/07/2023
Cybersecurity Framework v2.0	The NIST Cybersecurity Framework 2.0 Draft, Version 2.0	Draft	08/08/2023
SSDF	Secure Software Development Framework (SSDF): Recommendations for Mitigating the Risk of Software Vulnerabilities, Version 1.1	Final	02/03/2022
SP 800-213A	IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog, Final	Final	11/01/2021
NISTIR 8259B	IoT Non-Technical Supporting Capability Core Baseline, Final	Final	08/25/2021

Fig. 3. CPRT Catalog

The CPRT project is in its initial phase as of this writing. The initial phase involves developing the data format and freeing the data from a selection of our guidelines and frameworks that have broad impact. NIST will continue to collaborate with the public to ensure that access to our community-developed resources is manageable, streamlined, and usable — and CPRT is a big step in this direction. Comments, questions, and feedback can be sent to cprt@nist.gov. For more information on CPRT and its future phases, visit https://csrc.nist.gov/Projects/cprt.

3. Using the OLIR Catalog

This section provides information on how you can use the OLIR Catalog. Section 3.1 reviews the interfaces for viewing and searching the OLIRs in the Catalog, as well as the supporting information that the Catalog holds for each OLIR. Section 3.2 provides information on the DRM Analysis Tool that helps characterize relationships between Reference Documents. Section 3.3 explains how to generate on-screen reports between OLIRs, and Section 3.4 discusses how to download reports in multiple formats. Finally, Section 3.5 explores an additional use case for the OLIR Catalog: inferring additional relationships between Reference Documents based on authoritative OLIRs.

3.1. Searching the OLIR Catalog

The OLIR Catalog[1] contains all of the Reference Data – OLIR data and DRMs – for the National OLIR Program. All Reference Data in the OLIR Catalog have been validated against the requirements of NIST IR 8278A [2] and is displayed according to the most recent OLIR received. The OLIR Catalog provides an interface for viewing OLIRs and analyzing Reference Data.

The OLIR Catalog includes links to draft content that is being evaluated during a 30-day public comment period and final versions that have completed the public comment period. Following the public comment adjudication period, draft content is replaced with the final version, and the draft content is removed from the catalog.

Selecting the “More Details” link of an OLIR in the Catalog will display a description page, shown in Fig. 4, that includes the General Information of an OLIR.

[1] See https://csrc.nist.gov/projects/olir/informative-reference-catalog.

Framework_v1.1-to-SP800_221A (1.0.0) Informative Reference Details

Information and Communications Technology (ICT) Risk Outcomes

Download Informative Reference Resource

https://csrc.nist.gov/CSRC/media/Projects/olir/documents/submissions/Draft_Framework_v1.1-to-SP800_221A.xlsx

Informative Reference Information

Status:
Work-In-progress Draft

Informative Reference Version:
1.0.0

Focal Document Version:
SP 800-221A

Summary:
A mapping of NIST SP 800-221A content to the NIST Cybersecurity Framework version 1.1

Target Audience:
The primary audience for this publication includes both Federal Government and non-Federal Government professionals at all levels who understand Information and Communication Technology (ICT) but may be unfamiliar with the details of Enterprise Risk Management (ERM)

Comprehensive:
No

Comments:
N/A

Point of Contact:
ictrm@nist.gov

Category of Submitter:
Public Sector

Citations:
N/A

SHA3-256

641a537cc1b5c1ef61238af90d9737c24815c0c26d1bd17620cc5e7eadba2e47

AUTHORITY

Owner

Reference Document Author:
National Institute of Standards and Technology

Reference Document:
Framework for Improving Critical Infrastructure Cybersecurity

Reference Document Date:
04/16/2018

Reference Document URL:
https://csrc.nist.gov/publications/detail/white-paper/2018/04/16/cybersecurity-framework-v11/final

Reference Developer:
National Institute of Standards and Technology

Posted Date:
2022-07-20

Fig. 4. OLIR More Details Page

Table 1 lists fields and descriptions of the information depicted on the More Details page in Fig. 4.

Table 1. OLIR More Details Description Fields

Field Name	Description
Informative Reference Name	The name by which the OLIR listing will be known. The format is a human-readable string of characters.
Focal Document	A source document that is used as the basis for comparing a concept with a concept from another document
Web Address	The Uniform Resource Locator (URL) where the OLIR can be found

Field Name	Description
Status	Indicates the current status of the OLIR: • **Work-in-progress draft:** It is currently in an early stage of development and is incomplete. It has not been extensively edited or vetted. Work-in-progress drafts are solely informational in nature and are not intended to be implemented. • **Preliminary draft:** It is considered stable, but changes are expected to occur. There are gaps in the content, and the document is still incomplete. Early adopters may consider experimenting with the content with the understanding that they will identify gaps and challenges. • **Draft:** It is a complete draft proposed as a candidate for Final status. Changes may occur based on public comments, but such changes are expected to be relatively minor. Early adopters may attempt to use the content. • **Final:** Comments from the public comment period have been addressed, and the Informative Reference has been published as final.
Informative Reference Version	The version of the OLIR itself. The format is a string following the pattern: [major].[minor].[administrative]. The initial submission has an Informative Reference Version of 1.0.0.
Focal Document Version	The Focal Document version used in creating the OLIR
Summary	The purpose of the OLIR
Target Audience	The intended audience for the OLIR
Comprehensive	Whether the OLIR maps *all* Reference Document elements to the Focal Document ("Yes") or not ("No")
Comments	Notes to NIST or implementers
Point of Contact	At least one person's name, email address, and/or phone number within the OLIR Developer's organization
Category of Submitter	The category type of the OLIR: • **Public sector:** A governmental or regulatory agency, bureau, or board of the United States (federal, state, local) • **Private sector:** Any incorporated group that provides products, services, or information that cover topics related to the Focal Document • **Academia:** Informative references that originate from educational institutions, such as universities, colleges, and research laboratories • **Other:** Informative references that do not fall into the previous categories, such as standards development organizations and international governments
Citations	A list of source material (beyond the Reference Document) that supported development of the OLIR
SHA3-256	The hash value checksum that is generated between the validated OLIR sent to the OLIR Program and the publicly available OLIR. The value is monitored to maintain data integrity of the OLIR.
Authority	The organization responsible for authoring the OLIR in relation to the organization that produced the Reference Document represented by the OLIR submission
Reference Document Author	The organization(s) and/or person(s) that published the Reference Document
Reference Document	The full Reference Document name and version that is being compared to the Focal Document
Reference Document Date	The date that the Reference Document was published and, if applicable, amended
Reference Document URL	The URL where the Reference Document can be viewed, downloaded, or purchased

Field Name	Description
Reference Developer	The organization(s) that created the OLIR
Posted Date	The date that a validated OLIR submission was added to the catalog for the draft public comment period or the final posting following the completion of the public comment period and adjudication process

Figure 5 shows the OLIR Catalog Page where you can browse and search for OLIR content in multiple ways. You can search the entire OLIR Catalog to locate and retrieve an OLIR using a variety of fields, such as Informative Reference Name, Reference Document, Posted Date, Status, Submitting Organization, Authority, and Category of Submitter. Utilizing the dropdowns in the *Advanced Search* section, you can search OLIRs based on a Focal Document of your choice. You can also locate and retrieve an OLIR using a variety of fields, such as the type of Authority or Category of Submitter that an OLIR is catalogued as. Additionally, you can perform keyword searches of catalog content and sort the catalog columns within the table in a variety of different ways.

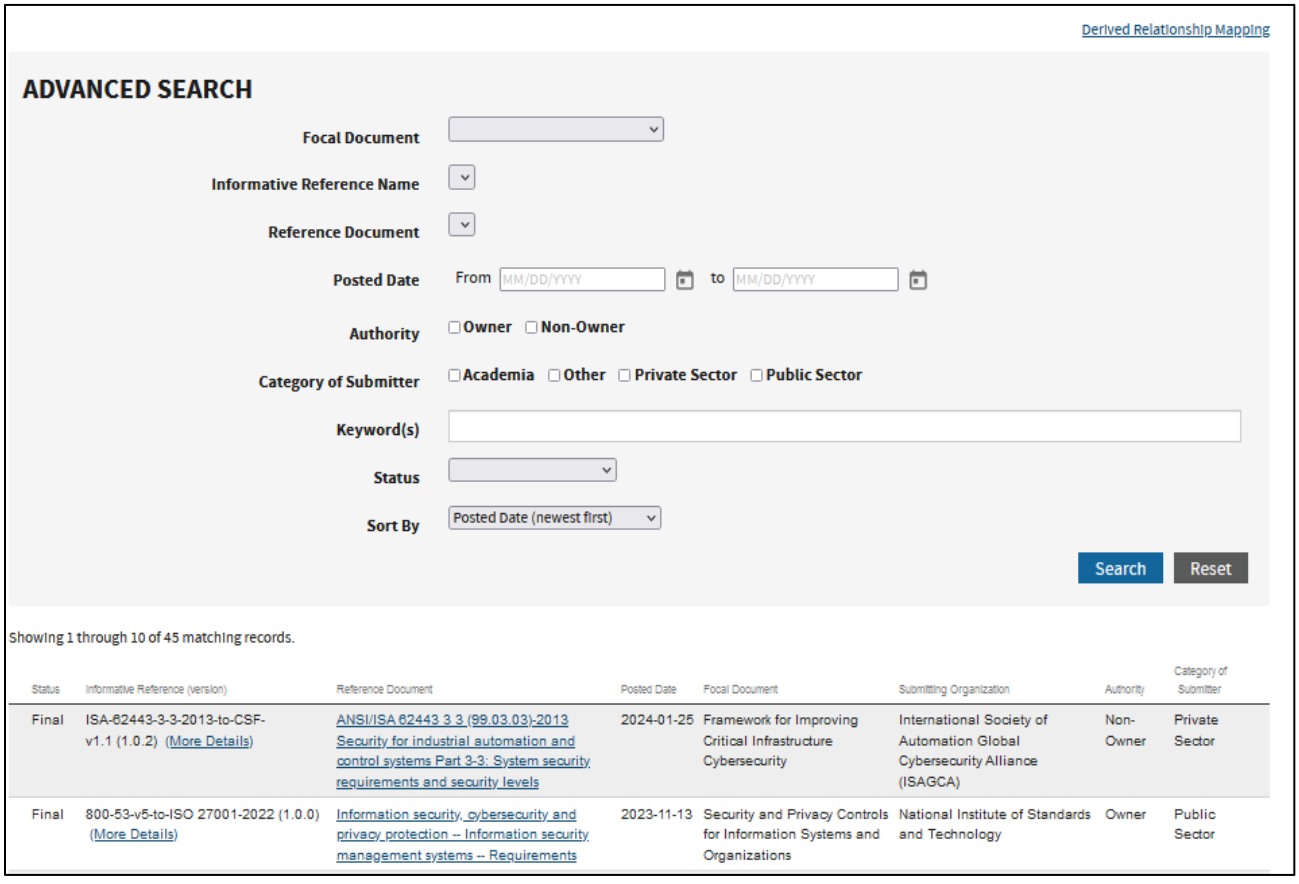


Fig. 5. OLIR Catalog Page

3.2. Using the Cross-Reference Comparison Reporting Tool

This OLIR analysis tool[2] allows users to view and generate DRMs in several ways. Users can select from the three template types (Concept Crosswalk, Set Theory, Supportive) and explore the NIST Focal Documents (NIST Publications), Developers (Cross-Reference Creators), and References associated with each template. DRMs are non-authoritative and represent a starting point when attempting to compare Reference Documents. Figure 6 depicts the homepage of the Cross-Reference Comparison Reporting Tool.

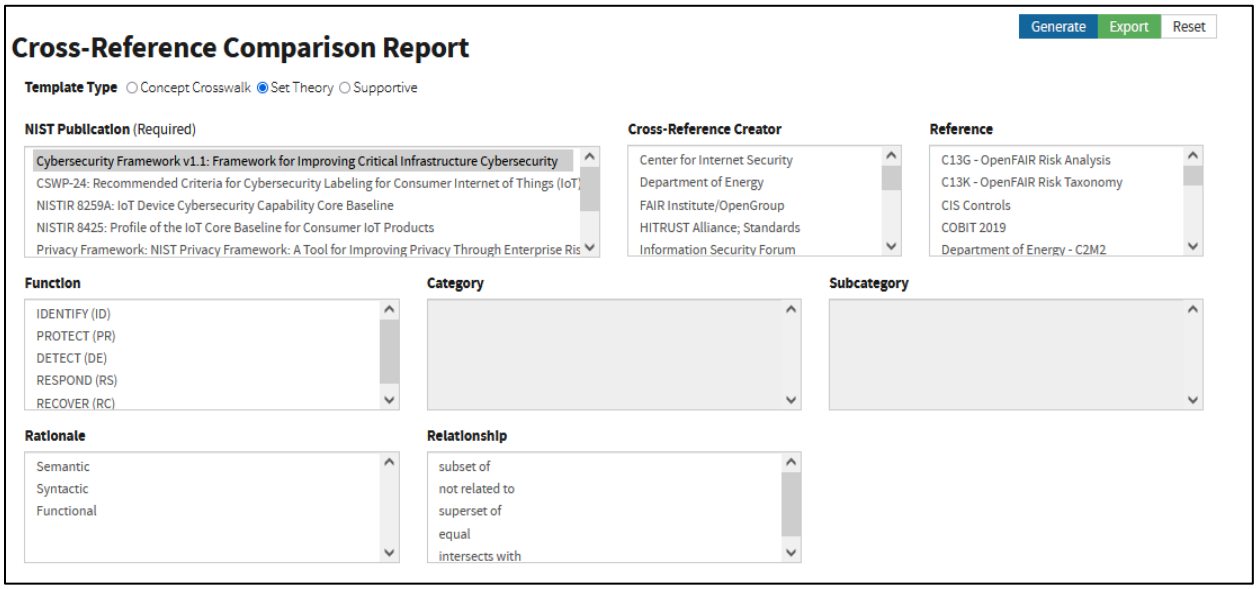


Fig. 6. Cross-Reference Comparison Report Tool Home Page

As Fig. 6 shows, when accessing the DRM Analysis tool, you first select the Template Type for comparative analysis. When generating a report, only one Focal Document is selectable at a time. You can display potential relationships for as many References that are available for a given Focal Document by selecting all References in the table. To select multiple References on a Windows computer, you can hold the "Ctrl" key. On a macOS computer, you can hold the "Command" key instead. By selecting the "More Filters" button, you can generate reports at any level of the Cybersecurity Framework Focal Document (i.e., Function, Category, Subcategory) or the SP 800-53 Focal Document (i.e., Control Family, Security/Privacy Control, Security Control Enhancements). Supplementary filtering is available dependent on the Template Type. For example, Fig. 6 displays the filtering capabilities for the Rationale and Relationship elements of the Set Theory template.

Additionally, in Fig. 7, the tool allows users to select any Focal Document, Developer, or Reference of their choosing, and the tool will filter and display associations based on their choice. For example, in Fig. 7, a user selects the Set Theory template type and selects the "National Institute of Standards and Technology" Developer. The tool filters and displays all Set

[2] See https://csrc.nist.gov/Projects/olir/Coverage-Report#/olir/coverage-report

Theory OLIRs where the developer was the National Institute of Standards and Technology, all applicable Focal Documents used by Developers for Set Theory OLIRs, and all the Set Theory OLIRs mapped to those Focal Documents.

Fig. 7. Cross-Reference Sorting

From this view, Fig. 8 shows that a user can then select a specific Focal Document (i.e., Privacy Framework), and all applicable References within the Set Theory template type that were developed by NIST will be displayed.

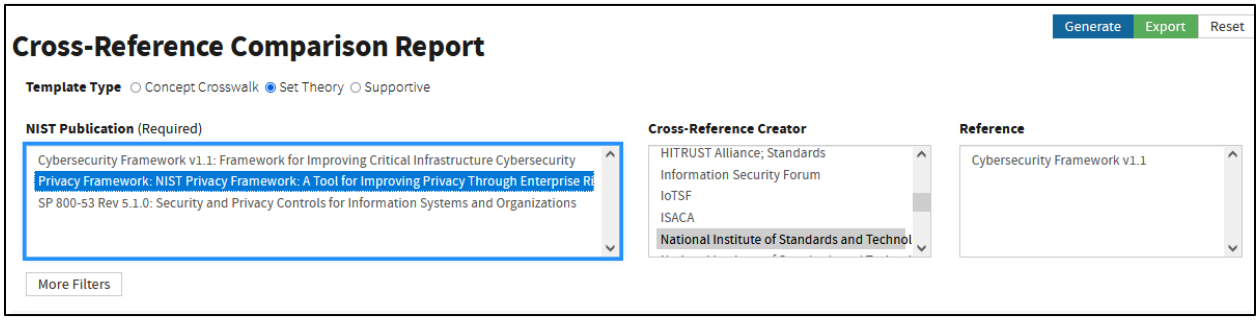
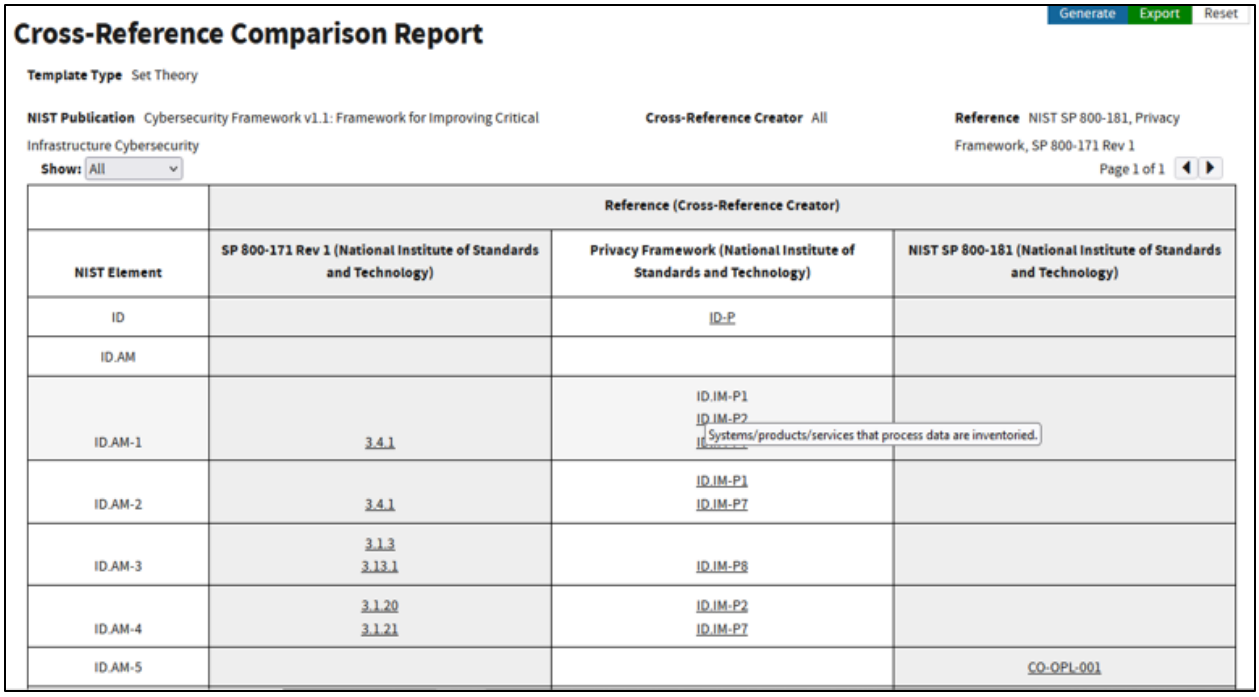


Fig. 8. Additional Sorting

When you access this page, all rationale and relationship pairings (except for the "not related to" relationship) are pre-selected by default. To filter and search for any specific rationale or relationship selections, select the More Filters button, and select the rationale or relationship as appropriate before generating a report.

3.3. Generating a Comparison Report

After selecting one Focal Document and one or more References, the "Generate" option (see Fig. 8) will become highlighted for selection. After selecting Generate, you are presented with an on-screen output table. Figure 9 shows the results of comparing three Set Theory References with the Cybersecurity Framework Focal Document selected. This on-screen output is the *Comparison Report.*



Cross-Reference Comparison Report

Generate | Export | Reset

Template Type Set Theory

NIST Publication Cybersecurity Framework v1.1: Framework for Improving Critical Infrastructure Cybersecurity

Cross-Reference Creator All

Reference NIST SP 800-181, Privacy Framework, SP 800-171 Rev 1

Show: All

Page 1 of 1

	Reference (Cross-Reference Creator)		
NIST Element	**SP 800-171 Rev 1 (National Institute of Standards and Technology)**	**Privacy Framework (National Institute of Standards and Technology)**	**NIST SP 800-181 (National Institute of Standards and Technology)**
ID		ID-P	
ID.AM			
ID.AM-1	3.4.1	ID.IM-P1 ID.IM-P2 Systems/products/services that process data are inventoried.	
ID.AM-2	3.4.1	ID.IM-P1 ID.IM-P7	
ID.AM-3	3.1.3 3.13.1	ID.IM-P8	
ID.AM-4	3.1.20 3.1.21	ID.IM-P2 ID.IM-P7	
ID.AM-5			CO-OPL-001

Fig. 9. Comparison Report Display

The Comparison Report presents the results according to the Focal Document element. For example, the Focal Document element identifier ID.AM-1 is shown in the leftmost column. The SP 800-171 Rev. 1 Reference in the 2nd column on the left displays a relationship pairing of 3.4.1. The Privacy Framework Reference in the middle column displays three relationships pairings of ID.IM-P1, ID.IM-P2, ID.IM-P7, and the rightmost column — SP 800-181 — displays no relationship pairings to the ID.AM-1 Focal Document Element.

"Tool Tips" are provided with descriptions of the reference elements (e.g., ID-IM-P1) when you scroll the pointer over the column headers. Figure 9 shows an example of a Tool Tip when hovering above an Element. Likewise, the Cybersecurity Framework Core definitions are displayed using the same Tool Tips behavior when you hover over the Focal Document Element identifier displayed in the leftmost column.

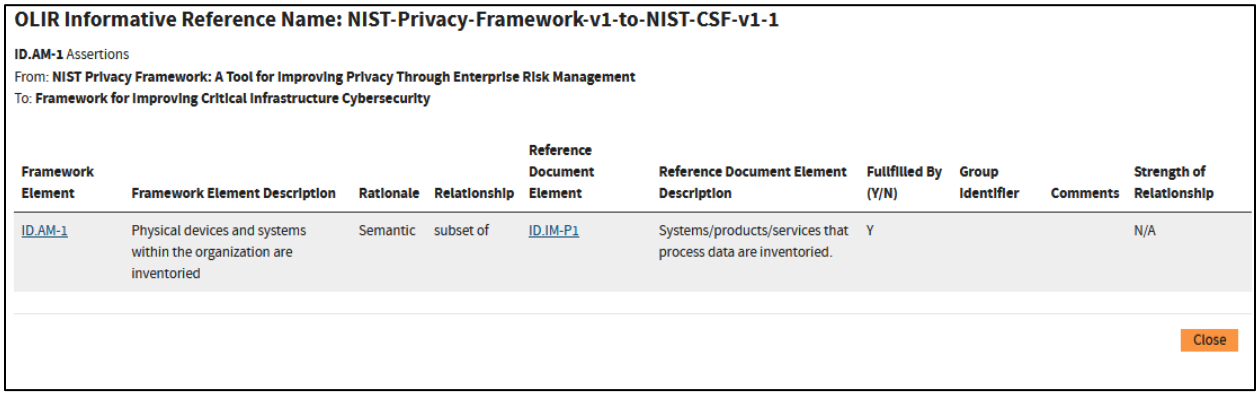
Table 2 provides a detailed description of the Comparison Report column headers.

Table 2. Comparison Report Column Header Descriptions

Field Name	Description
NIST Element	The identifier of the Focal Document Element being mapped
Reference	The name by which the Informative Reference listing will be referred
Cross-Reference Creator	A person, team, or organization that creates an OLIR and submits it to the National OLIR Program.

Within Fig. 9, Reference Document Elements displayed within the Comparison Report (e.g., ID.IM-P1) include links to that provide additional OLIR information about a specific relationship pairing. For example, when a user selects ID.IM-P1 from the Privacy Framework Reference

within the middle column of the ID.AM-1 focal document row, a pop-up window will display the specific relationship information between these two elements. Figure 10 details this information.



OLIR Informative Reference Name: NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1

ID.AM-1 Assertions
From: **NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management**
To: **Framework for Improving Critical Infrastructure Cybersecurity**

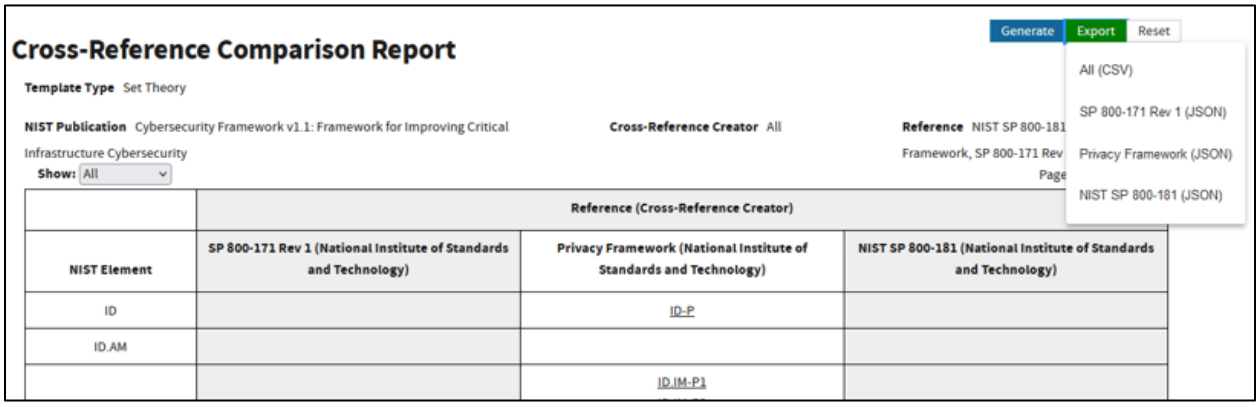
Framework Element	Framework Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Group Identifier	Comments	Strength of Relationship
ID.AM-1	Physical devices and systems within the organization are inventoried	Semantic	subset of	ID.IM-P1	Systems/products/services that process data are inventoried.	Y			N/A

Close

Fig. 10. OLIR Element Data

3.4. Downloading a Report

After creating a Comparison Report, multiple report download options are available, as depicted in the right corner of Fig. 11. Within "Export" are links for CSV (comma-separated values) and JSON report files.[3] Clicking on the corresponding CSV or JSON format will download the file. The report downloads provide for more convenient human comparison and automated processing.[4]



Cross-Reference Comparison Report

Generate | Export | Reset

All (CSV)
SP 800-171 Rev 1 (JSON)
Privacy Framework (JSON)
NIST SP 800-181 (JSON)

Template Type Set Theory

NIST Publication Cybersecurity Framework v1.1: Framework for Improving Critical Infrastructure Cybersecurity

Cross-Reference Creator All

Reference NIST SP 800-181 Framework, SP 800-171 Rev

Page

Show: All

	Reference (Cross-Reference Creator)		
NIST Element	**SP 800-171 Rev 1 (National Institute of Standards and Technology)**	**Privacy Framework (National Institute of Standards and Technology)**	**NIST SP 800-181 (National Institute of Standards and Technology)**
ID		ID-P	
ID.AM			
		ID.IM-P1	

Fig. 11. Report Download Options

Figure 12 represents a sample CSV report. This is a common format that is easily ingested into a spreadsheet program where searching and sorting functions can be performed. Those functions are not available via the Cross-Reference Comparison Tool.

[3] The CSV and JSON download links are only available after the Comparison Report is generated.
[4] See NIST IR 8278A [2] for additional field descriptions.

	A	B	C	D
1	References	SP 800-171 Rev 1	Privacy Framework	NIST SP 800-181
2	Cross-Reference Creator	National Institute of Standards a	National Institute of Standards and	National Institute of Standards and Technology
3	ID		ID-P	
4	ID.AM			
5	ID.AM-1	3.4.1	ID.IM-P1, ID.IM-P2, ID.IM-P7	
6	ID.AM-2	3.4.1	ID.IM-P1, ID.IM-P7	
7	ID.AM-3	3.1.3, 3.13.1	ID.IM-P8	
8	ID.AM-4	3.1.20, 3.1.21	ID.IM-P2, ID.IM-P7	
9	ID.AM-5			CO-OPL-001
10	ID.AM-6		GV.PO-P3	OV-SPP-001, CO-CLO-001
11	ID.BE		ID.BE-P	
12	ID.BE-1		ID.BE-P1	OV-MGT-002, OV-SPP-001, OV-EXL-001
13	ID.BE-2			OV-MGT-002, OV-SPP-001, OV-EXL-001, CO-OPL-001
14	ID.BE-3		ID.BE-P2	OV-MGT-002, OV-SPP-001, OV-EXL-001

Fig. 12. Sample CSV Report

The JSON format provides the report data in a format that many tools can utilize to perform more in-depth analyses that are not available using the Cross Reference Comparison Tool. The JSON file depicted in Fig. 13 shows how the data are displayed.


```
{
    "data": {
        "response": {
            "elements": {
                "$id": "https://csrc.nist.gov/csrc/media/projects/cprt/documents/schema/cprt_schema.json",
                "$schema": "https://json-schema.org/draft/2020-12/schema",
                "documents": [
                    {
                        "doc_identifier": "NIST-PRIVACY-FRAMEWORK-V1-TO-NIST-CSF-V1-1",
                        "name": "NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1",
                        "version": "1.0.0",
                        "website": "https://www.nist.gov/document/privacy-framework-olir"
                    },
                    {
                        "doc_identifier": "CSF_1_1_0",
                        "name": "Framework for Improving Critical Infrastructure Cybersecurity",
                        "version": "Version 1.1",
                        "website": "https://csrc.nist.gov/publications/detail/white-paper/2018/04/16/cybersecurity-framework-v11/final"
                    },
                    {
                        "doc_identifier": "PF_1_0_0",
                        "name": "NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management",
                        "version": "Version 1.0",
                        "website": "https://csrc.nist.gov/publications/detail/white-paper/2020/01/16/nist-privacy-framework-version-10/final"
                    },
                    {
                        "doc_identifier": "NISTIR_8278_1_0_0",
                        "name": "National Online Informative References (OLIR) Program",
                        "version": "",
                        "website": "https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8278.pdf"
                    }
                ],
                "elements": [
                    {
```


Fig. 13. Sample JSON Report

3.5. Inferring Additional Relationships Between Reference Documents

The Comparison Report and report download options provide a convenient way to quickly view how one Reference Document may relate to another by leveraging a Focal Document that they have in common. The Cross-Reference Comparison Tool automates the brute-force comparison method for analyzing Reference Documents and renders transitive relationship possibilities for the analyst to consider. The Cross-Reference Comparison Tool output only displays authoritative relationships. If you compare the relationships from different Reference Documents and infer additional relationships among them, those inferred — *derived* — relationships are non-authoritative. However, they are still useful because they represent a starting point for various types of comparative analysis and research.

With much of the relationship data defined by the OLIR Developer already, you can simply generate a full report between two Reference Documents and export the data output in CSV format to import it into a spreadsheet application for searching and sorting reference data. For example, once the CSV file is imported, you can sort the reference data by Functions, Categories, and Subcategories or Control Families, Security/Privacy Controls, or Security Control Enhancements (depending on the Focal Document selected.)

To narrow the potential for identifying strong associations between Reference Documents, you could generate a Comparison Report using the Rationale and Relationship selectors to indicate association strength. By selecting options such as “semantic” and “equal to,” you can parse the Comparison report for Reference relationships that have a better chance of relevance than, for example, what the options of “functional” and “intersection” might provide.

Another popular use case involves conducting a gap analysis between documents. Here are some examples:

- If you know your organization already implements the NIST Privacy Framework, and NIST publishes a new version of SP 800-171, you can generate a Comparison Report selecting the “not related to” Relationship option for Set Theory OLIRs. This report may contain data that are unrelated to the NIST Cybersecurity Framework, but it does not preclude the data from relating to other Reference Documents. Just because SP 800-171 and the Privacy Framework have elements that do not map to the Cybersecurity Framework does not mean that the two Reference Documents are unrelated to each other.
- You could generate Comparison Reports in order to identify significant changes between two versions of the same document. First, you could report on the relationships between the Privacy Framework and the current version of SP 800-171. Next, you could report on the relationships between the Privacy Framework and a new draft revision of SP 800-171. Finally, you could use a tool to compare those two reports and identify their differences.
- You could identify the gaps that would need to be addressed if your organization adopted a new security framework by generating a Comparison Report comparing the Reference Documents that the organization already complies with to the Reference Document for the new security framework.

A final gap analysis example involves a vendor of cybersecurity products and services. Such a vendor could generate a Comparison Report that shows which requirements from Reference Documents their products and services help to address. This provides a starting point for conducting additional analysis for each identified requirement to determine the strength of each relationship.

As additional use cases are identified for using the OLIR Catalog, they will be added to this section of the document.

References

[1] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0 (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.29

[2] Barrett M, Keller N, Quinn S, Smith MC, Scarfone K, Johnson V (2024) National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) 8278A Revision 1. https://doi.org/10.6028/NIST.IR.8278Ar1

[3] National Institute of Standards and Technology (2020) The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0 (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.10

[4] Fagan MJ, Megas KN, Scarfone KA, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259A. https://doi.org/10.6028/NIST.IR.8259A

[5] Joint Task Force Transformation Initiative (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[6] Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2. https://doi.org/10.6028/NIST.SP.800-171r2

[7] Scarfone KA, Souppaya M, Fagan M (2024) Mapping Relationships Between Documentary Standards, Regulations, Framework, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) 8477. https://doi.org/10.6028/NIST.IR.8477

Appendix A. List of Symbols, Abbreviations, and Acronyms

CPRT
Cybersecurity and Privacy Reference Tool

CSV
Comma-Separated Values

DRM
Derived Relationship Mapping

FOIA
Freedom of Information Act

ICT
Information and Communications Technology

IoT
Internet of Things

IR
Internal Report

ITL
Information Technology Laboratory

JSON
JavaScript Object Notation

NIST
National Institute of Standards and Technology

OLIR
Online Informative References

SME
Subject Matter Expert

SP
Special Publication

URL
Uniform Resource Locator

USG
United States Government

Appendix B. Glossary

Concept Crosswalk OLIR
An OLIR that indicates relationships between pairs of elements without additional characterization of those relationships.

Concept Relationship Style
An explicitly defined convention for characterizing relationships for a user case. OLIR supports three concept relationship styles: concept crosswalk, set theory relationship mapping, and supportive relationship mapping.

Derived Relationship Mapping
A potential mapping between Reference Document Elements identified by finding elements from two or more Reference Documents that map to the same Focal Document Element.

Developer
See *OLIR Developer*.

Focal Document
A NIST document that is used as the basis for comparing its elements with elements from another document. Examples of Focal Documents include the Cybersecurity Framework version 2.0, the Privacy Framework version 1.0, and SP 800-53 Revision 5.

Focal Document Element
A discrete section, sentence, phrase, or other identifiable piece of content from a Focal Document.

Informative Reference
See *Online Informative Reference*.

Informative Reference Developer
See *OLIR Developer*.

Non-Owner
An OLIR produced by anyone other than the owner of the Reference Document.

OLIR Catalog
The National OLIR Program's online site for sharing OLIRs.

OLIR Developer
A person, team, or organization that creates an OLIR and submits it to the National OLIR Program.

Online Informative Reference
Relationships between elements of two documents that are recorded in a NIST IR 8278A-compliant format and shared by the OLIR Catalog. There are three types of OLIRs: concept crosswalk, set theory relationship mapping, and supportive relationship mapping.

Owner
An OLIR produced by the owner of the Reference Document.

Reference
See *Online Informative Reference*.

Reference Document
A document being compared to a Focal Document, such as traditional documents, products, services, education materials, and training.

Reference Document Element
A discrete section, sentence, phrase, or other identifiable piece of content from a Reference Document.

Set Theory Relationship Mapping OLIR
An OLIR that characterizes each relationship between pairs of elements by qualifying the rationale for indicating the connection between the elements and classifying the relationship based on set theory principles.

Strength of Relationship
The extent to which a Reference Document Element and a Focal Document Element are similar.

Supportive Relationship Mapping OLIR
An OLIR that indicates how a supporting concept can or does help achieve a supported concept, with one of the concepts being a Focal Document Element and the other a Reference Document Element.

User
A person, team, or organization that accesses or otherwise uses an OLIR.

Appendix C. Change Log

For the final version of Revision 1 (NIST IR 8278r1), the following changes were made to this report:

- Reformatted all content to follow the latest NIST technical report template
- Updated content throughout the report to reflect recent changes to OLIR, such as adding the addition of the Supportive Relationship type, and updated screenshots of the OLIR program tools and reports.
- Section 2.3 – Expanded on the NIST Cybersecurity and Privacy Reference Tool (CPRT) content

In the public comment draft of Revision 1 (NIST IR 8278r1), the following changes were made to this report:

- Reorganized the content and made editorial changes throughout the report to improve clarity and usability
- Reformatted all content to follow the latest NIST technical report template
- Updated content throughout the report to reflect recent changes to OLIR, such as eliminated the tiers concept for reference data and added the concept of unilateral and bilateral OLIRs
- Section 2.3 – Created new subsection on the NIST Cybersecurity and Privacy Reference Tool (CPRT)