Withdrawn Draft

Withdrawal Date	November 20, 2020
Original Release Date	August 4, 2020

Superseding Document

Status	Final
Series/Number	NIST Interagency or Internal Report 8278
Title	National Cybersecurity Online Informative References (OLIR) Program: Program Overview and OLIR Uses
Publication Date	November 2020
DOI	https://doi.org/10.6028/NIST.IR.8278
CSRC URL	https://csrc.nist.gov/publications/detail/nistir/8278/final
Additional Information	OLIR homepage: https://csrc.nist.gov/projects/olir

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

Draft (2nd) NISTIR 8278

National Cybersecurity Online Informative References (OLIR) Program:

Program Overview and OLIR Uses

Nicole Keller
Stephen Quinn
Karen Scarfone
Matthew Smith
Vincent Johnson

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8278-draft2

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

Draft (2nd) NISTIR 8278

National Cybersecurity Online Informative References (OLIR) Program:

Program Overview and OLIR Uses

Nicole Keller
Stephen Quinn
Computer Security Division
Information Technology Laboratory

Matthew Smith
Huntington Ingalls Industries
Annapolis Junction, MD

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

Vincent Johnson
Electrosoft Services, Inc.
Reston, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8278-draft2

August 2020

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

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

National Institute of Standards and Technology Interagency or Internal Report 8278
31 pages (August 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8278-draft2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: ***August 4, 2020*** **through** ***September 4, 2020***

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

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

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL’s responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

The National Cybersecurity Online Informative References (OLIR) Program is a NIST effort to facilitate subject matter experts in defining standardized Online Informative References (OLIRs), which are relationships between elements of their documents and elements of other documents like the NIST Cybersecurity Framework. The OLIR Program provides a standard format for expressing OLIRs as well as a centralized location for displaying them. This report describes the OLIR Program, focusing on explaining what OLIRs are, what benefits they provide, how anyone can search and access OLIRs, and how subject matter experts can contribute OLIRs.

Keywords

catalog; Cybersecurity Framework; informative references; mapping; National Cybersecurity OLIR Program; Online Informative References (OLIRs).

Acknowledgments

Thanks to all of those who contributed to or commented on this document.

Audience

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

Trademark Information

All registered trademarks and trademarks belong to their respective organizations.

Note to Readers

As of this writing, NIST plans on soon providing downloaded Javascript Object Notation (JSON) formats for the three focal document templates (Cybersecurity Framework version 1.1, the Privacy Framework version 1.0, and Special Publication 800-53 Rev. 4) and all current NIST-developed OLIRs within the OLIR Catalog.

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: olir@nist.gov

Executive Summary

The fields of cybersecurity, privacy, and workforce have a large number of documents, such as standards, guidance, and regulations. There is no standardized way to indicate how an element of one document relates to an element of another document (e.g., the relationship between requirement A in one document and recommendation 7.2 in another document). This relationship is called an *informative reference*. The *Framework for Improving Critical Infrastructure Cybersecurity* ("Cybersecurity Framework") [1] introduced informative references, but these were simple prose mappings that only noted that a relationship existed and not the nature of that relationship. These informative references were also part of the Cybersecurity Framework document itself, so they could not be readily updated as the other documents changed.

The National Cybersecurity Online Informative References Program is a NIST effort to facilitate subject matter experts (SMEs) in defining standardized online informative references (OLIRs) between elements of their cybersecurity, privacy, and workforce documents and elements of other cybersecurity, privacy, and workforce documents like the Cybersecurity Framework. At this stage of the OLIR Program evolution, the initial focus is on relationships to cybersecurity and privacy documents.

The OLIRs are in a simple standard format defined by NIST Interagency or Internal Report (IR) 8278A, *National Cybersecurity Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers* ("NISTIR 8278A") [2], and they are displayed in a centralized location. By following this approach, cybersecurity document owners can use the OLIR Program as a mechanism for communicating with owners and users of other cybersecurity documents. Given the OLIR Program's decentralized nature, cybersecurity document owners also have the flexibility to update their documents and then update their OLIRs according to their own unique requirements and schedules.

The OLIR Program integrates ongoing NIST projects that respond to administrative and legislative requirements, including those for the Cybersecurity Framework under Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, [3] released in February 2013, and the Federal Information Security Modernization Act of 2014 [4], which amended the Federal Information Security Management Act of 2002 (FISMA). The OLIR Program also addresses many Office of Management and Budget (OMB) memoranda that address specific cybersecurity issues and comprise large sets of regulations with which organizations must comply. The OLIR Program can represent relationships to any authoritative documents, products, or services. These resources can be generated from national and international standards, guidelines, frameworks, and regulations to policies for individual organizations, sectors, or jurisdictions.

The purpose of this document is to describe the National Cybersecurity OLIR Program and explain the use, benefits, and management of the OLIR Catalog—the online location for sharing OLIRs—for both the SMEs contributing OLIRs to it and the Catalog's users. The content of this document complements that of NISTIR 8278A [2], which provides additional information for the SMEs defining OLIRs and submitting them to the OLIR Program. SMEs should read this document first, then NISTIR 8278A.

Table of Contents

Executive Summary ..... **v**
1 Introduction **1**
1.1 Purpose and Scope 1
1.2 Document Structure 1
2 Overview of the National Cybersecurity OLIR Program **2**
3 Common Uses of the OLIR Catalog **4**
3.1 Reference Data 4
3.1.1 Tier 1 – Informative References 7
3.1.2 Tier 2 – Derived Relationship Mappings (DRMs) 7
3.2 The OLIR Catalog 8
3.3 The DRM Analysis Tool 12
3.4 Display Report 13
3.5 Report Downloads 15
3.5.1 Report Download in CSV Format 16
3.5.2 Report Download in JSON Format 16
3.6 Common Use Cases 17
3.6.1 Comparative Analysis of Cybersecurity Documents and Controls 17
References **20**

List of Appendices

Appendix A— Acronyms **21**
Appendix B— Glossary **22**

List of Figures

Figure 1: Relationship Types 4
Figure 2: Relative Strength of Relationships 6
Figure 3: Multiple Documents Related to a Focal Document 8
Figure 4: OLIR Catalog Page 9
Figure 5: Informative Reference More Details Page 10
Figure 6: DRM Analysis Tool Home Page 12
Figure 7: Multi-Select Example 13
Figure 8: Display Report Example 14

Figure 9: Report Download Options 15
Figure 10: Sample CSV Report 16
Figure 11: Sample JSON Report 17

List of Tables

Table 1: Relationship Type Descriptions 5
Table 2: Informative Reference More Details Description Fields 10
Table 3: Display Report Column Header Descriptions 15

1 Introduction

1.1 Purpose and Scope

The purpose of this document is to describe the National Cybersecurity Online Informative References (OLIR) Program and explain the use and benefits of the OLIR Catalog for Informative Reference Developers ("Developers") and Informative Reference Users ("Users") of the OLIR Program.

In addition to this document, Developers may also be interested in NIST Interagency or Internal Report (IR) 8278A, *National Cybersecurity Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers* ("NISTIR 8278A") [2]. NISTIR 8278A is intended to assist Developers as they complete the spreadsheet template for submitting their OLIRs to the Program. Developers should read this document first, then NISTIR 8278A.

1.2 Document Structure

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

- Section 2 provides an overview of the OLIR Program.
- Section 3 describes common uses of the OLIR Catalog relevant to both Developers and Users.
- The References section lists the references for the publication.
- Appendix A contains acronyms used throughout the document.
- Appendix B provides a glossary of terminology used throughout the document.

2 Overview of the National Cybersecurity OLIR Program

In a general sense, an informative reference, sometimes called a mapping, indicates how one document relates to another document. Informative references were originally documented within the original version of the NIST Cybersecurity Framework document. While the concept of informative references was well received, the static nature of the Cybersecurity Framework document meant that some of its informative references became outdated as the documents they referenced were updated.

Within the context of the National Cybersecurity OLIR Program, an *Informative Reference* (abbreviated as *Reference)* indicates the relationship(s) between elements of two documents. The source document, called the *Focal Document*, is used as the basis for the document comparison. 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—either could be a product, service, training, etc. A *Focal Document element* or a *Reference Document element* is a discrete section, sentence, phrase, or other identifiable piece of content of a document.

As of this writing, the OLIR Program has three Focal Documents: the *Framework for Improving Critical Infrastructure Cybersecurity* ("Cybersecurity Framework") version 1.1 [1], the *Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* ("Privacy Framework") version 1.0 [5], and Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* ("SP 800-53 Rev. 4") [6].

Although using Informative References can significantly improve understanding of documents within organizations, using an Informative Reference does not demonstrate or certify that an organization complies with a document.

The OLIR Program provides an online site—the OLIR Catalog—for displaying, sharing, and comparing Informative References. The OLIR Program defines a simple format in NISTIR 8278A [2] for expressing References in the OLIR Catalog in a standardized, consistent manner. The OLIR Program offers several benefits, including the following:

- There are many potential Reference Documents, so the OLIR Program provides a single, easy-to-use place where people can obtain information on many Reference Documents and analyze their relationships. This approach also significantly reduces the time that organizations need to research and analyze their current and target cybersecurity activities and to communicate with others regarding those activities. Without a central location, finding and comparing cybersecurity resources can be difficult.
- The OLIR Program increases transparency, alignment, and harmonization of definitions and concepts across Reference Documents.
- Standardizing how References are expressed makes them more consistent, clear, usable, repeatable, and organizable, and it provides a way for automation technologies to ingest and utilize them.

- Having a centralized OLIR Program allows for the authentication of each Reference's source and identifies whether or not the Reference was provided by a verified SME on the Reference Document.
- The OLIR Program employs additional mathematic rigor (e.g., standard set theory principles, such as subset, superset, equal, intersect, and discrete logic) to express References instead of just relying on prose, which is ambiguous and subject to individual interpretation.
- The OLIR Program increases the integration of NIST guidance, which is produced in support of United States Government (USG) legislative and administrative responsibilities.

The OLIR Program also defines a formal process for vendors and other OLIR 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 the review, update, and maintenance of OLIRs as Focal and Reference Documents are updated and revised.

3 Common Uses of the OLIR Catalog

This section provides information on the use of the OLIR Catalog for both OLIR Developers and Users. Section 3.1 explains the types of information that the Catalog contains. Section 3.2 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 3.3 provides information on an analysis tool that helps characterize relationships among Reference Documents. Section 3.4 explains how to generate comparative analysis reports between OLIRs at different levels of abstraction, and Section 3.5 discusses how to download those reports. Finally, Section 3.6 introduces use cases for the OLIR Catalog.

3.1 Reference Data

The OLIR Catalog contains two types of information on the relationships between Focal Documents and Reference Documents: Informative References and Derived Relationship Mappings. These relationships are organized as *Reference Data* via the OLIR Catalog according to the vetting processes delineated in NISTIR 8278A [2] with the objective of providing transparency from the Informative Reference Developers for reproducibility and discussion by Users.

Each relationship between a Reference Document element and a Focal Document element has a *type*. The type indicates how the meanings of the two elements are related, and for each relationship, the type will be one of the following, as depicted in Figure 1 (where "f" is a Focal Document element and "r" is a Reference Document element) and further explained in Table 1.

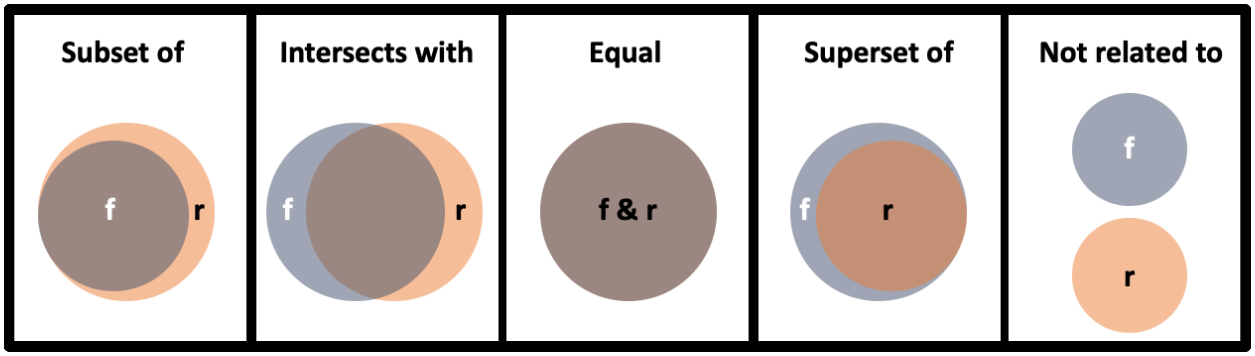


Figure 1: Relationship Types

Table 1: Relationship Type Descriptions

Relationship Type	Description
Subset of	The Focal Document element is a subset of the Reference Document element. In other words, the Reference Document element contains everything that the Focal Document element does and more.
Intersects with	The two elements have some overlap, but each includes content that the other does not.
Equal	The two elements are very similar (not necessarily identical).
Superset of	The Focal Document element is a superset of the Reference Document element. In other words, the Focal Document element contains everything that the Reference Document element does and more.
Not related to	The two elements do not have anything in common.

The explanation of why a Reference Document element and a Focal Document element are related is attributed to one of three basic reasons referred to as the *rationale*:

- **Syntactic** – Analyzes the linguistic meaning of the Reference Document element and the Focal Document element to develop the conceptual comparison sets. Syntactic analysis uses literal analysis of (i.e., translates) the Reference Document or Focal Document elements. For example, the following statements have identical syntax:

  printf (“bar”); [… C programming language]

  printf (“bar”); [… C programming language]

- **Semantic** – Analyzes the contextual meaning of the Reference Document element and the Focal Document element to develop the conceptual comparison sets. Semantic analysis interprets (i.e., transliterates) the language within the Reference Document or Focal Document elements. For example, the following statements convey the same semantic meaning:

  “Organization employs a firewall at the network perimeter”

  “The enterprise uses a device that has a network protection application installed to safeguard the network from intentional or unintentional intrusion.”

- **Functional** – Analyzes (i.e., transposes) the functions of the Reference Document element and the Focal Document element to develop the conceptual comparison sets. For example, the following statements result in the same functional result of the word ‘foo’ printing to the screen:

  printf (“foo\n”); [… C programming language]

  print “foo” [… BASIC programming language]

Subject matter experts already make assertions implicitly based on the relationship type and the rationale but are not always aware that they are using these logical constructs. One of the goals of the OLIR Program is to further the science by encouraging explicit declarations of relationship types and rationales for assertions.

Another goal of the OLIR Program is to find ways to quantify the strength of a relationship, which would help enable evaluating a relationship between two elements of different sizes. Figure 2 illustrates how a single relationship type can encompass relationships of different strengths. Case 1 shows a Focal Document element and a Reference Document element in a Subset relationship with many common elements, while Case 2 shows a Subset relationship where the two elements have fewer common elements. The OLIR Program encourages subject matter experts making assertions to include a measure of the strength of comparable relationships but does not prescribe a particular methodology for doing so.

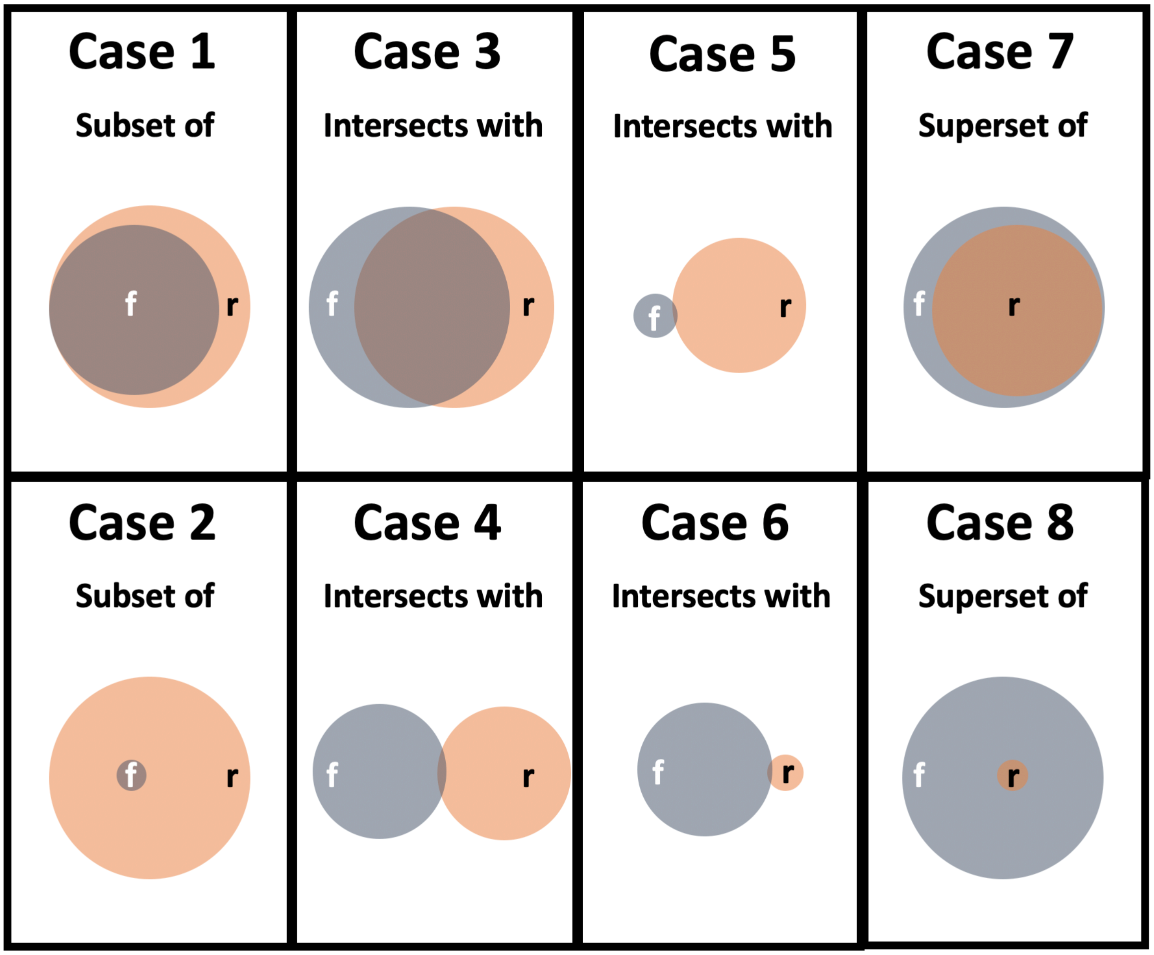


Figure 2: Relative Strength of Relationships

Quantifying the strength of a relationship for an Informative Reference is optional, and its omission should not be interpreted as negative. It is intended for lateral comparisons only, like the Cybersecurity Framework and the Privacy Framework, and not comparisons of documents at different levels, such as the Cybersecurity Framework and a research paper on a topic in quantum cryptography. Non-lateral relationships are to be designated with "N/A."

3.1.1 Tier 1 – Informative References

Tier 1 Reference Data are Informative References that have been vetted with respect to NIST documents by NIST staff, submitted for a public comment period, and finalized. The OLIR Program has two major groups of References:

- **Owner:** These are produced by the owner of the Reference Document. For example, NIST is the owner of NIST SP 800-171 [7] and produced the Informative Reference for SP 800-171; therefore, the designation of "owner" is granted to the SP 800-171 Informative Reference developed by NIST.
- **Non-Owner:** These are produced by anyone who is NOT the Reference Document owner. For example, if Organization A developed an Informative Reference for SP 800-171, the Informative Reference would be designated "non-owner."

Creating Informative References will not only provide more consistency in cybersecurity communication among federal agencies but also provide a much more cost-effective method for establishing and verifying the relationships between Reference Documents through Focal Documents. NIST encourages Reference Document owners, software vendors, service providers, educators, and other parties to develop and submit References to the OLIR Program.

When multiple Informative References are available for a particular Reference Document, Users should take into consideration the sources of the Informative References. Generally, Informative References from owners can be used more consistently and efficiently than Informative References from non-owners. If it is not clear which Informative Reference should be analyzed based on the authority of the submission (owner/non-owner), Users should focus on the quality and completeness of the Informative Reference Developer.

3.1.2 Tier 2 – Derived Relationship Mappings (DRMs)

Tier 2 Reference Data are the Derived Relationship Mappings (DRMs). DRMs are the result of using the relationships between Reference Documents and a Focal Document to make inferences about document-to-document relationships. Figure 3 depicts how a User could find 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 are dynamically generated when a User utilizes the DRM Analysis Tool to search the OLIR Catalog on the OLIR website, as described in Section 3.3. The results of the search are displayed to the User, as shown in Figure 8. DRMs serve as the foundation for gap and comparative analysis.

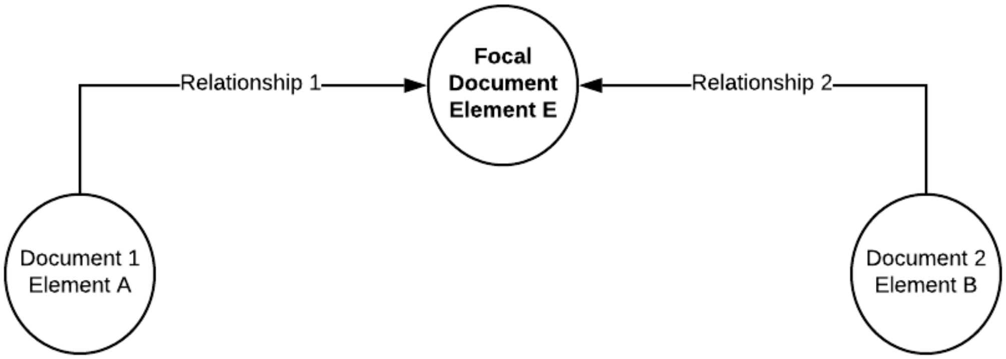


Figure 3: Multiple Documents Related to a Focal Document

The function of DRMs is to display relationships between Reference Documents and Focal Documents. While the inferences that a User makes while using DRMs are informative, they are not considered verified nor authoritative. DRMs help users of cybersecurity documents make informed decisions regarding cybersecurity risk management activities.

These relationships, which are defined in NISTIR 8278A [2], do not indicate the relationships among the Reference Documents. Therefore, in reference to Figure 3, 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.

Another caveat about 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 someone wants to compare Focal Document Element PR.AC-1, "Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes" [1], to Reference Document 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" [6]. The Focal Document Element is at a higher level than the Reference Document Element, which specifies, in detail, one part of what the Focal Document Element encompasses. For some DRMs, the difference in the level of detail of the elements being compared may be vast.

See Section 3.6 for common use cases for DRMs.

3.2 The OLIR Catalog

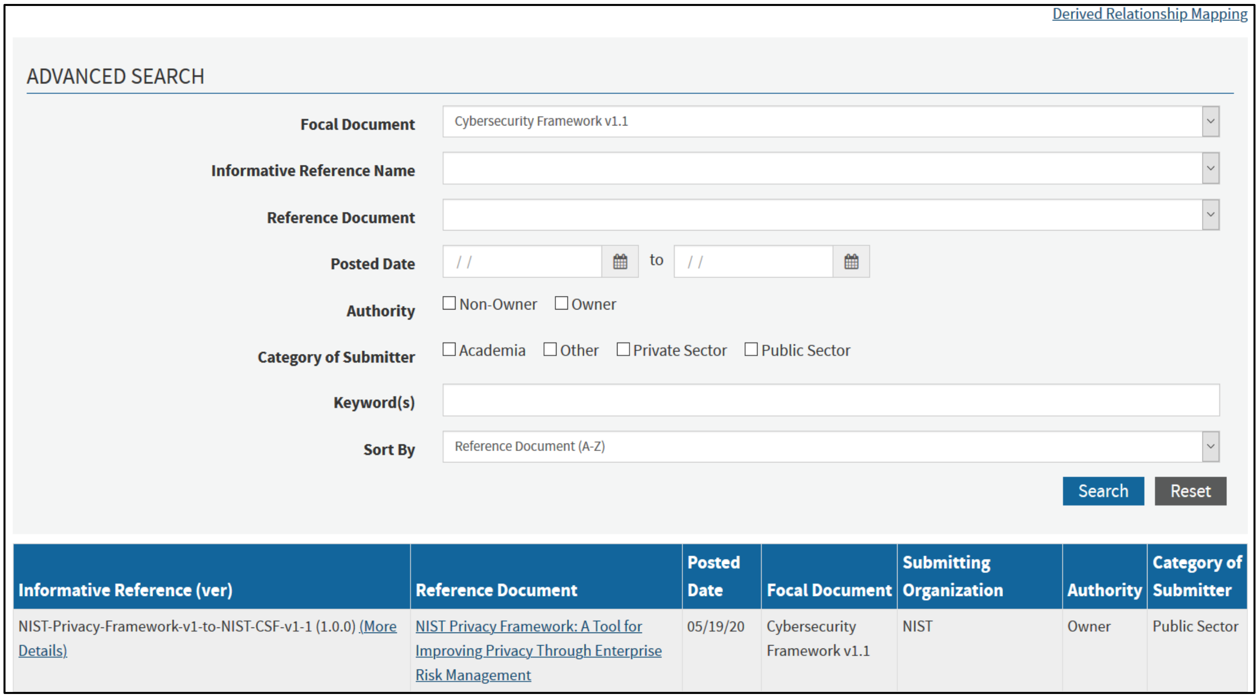
The OLIR Catalog[1] contains all of the Reference Data—Informative Reference data and DRMs—for the National Cybersecurity OLIR Program. All Reference Data in the OLIR Catalog has been validated against the requirements of NISTIR 8278A [2] and is displayed by default

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

according to the most recent OLIR received. The OLIR Catalog provides an interface for Developers and Users to view Informative References and analyze Reference Data.

The 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.

Figure 4 shows the OLIR Catalog Page. From this page, Users can browse and search Informative Reference content in multiple ways. Users can search the entire OLIR catalog to locate and retrieve an Informative Reference using a variety of fields, such as Informative Reference (name), Reference Document, Posted Date, and Submitting Organization. Utilizing the dropdowns in the *Advanced Search* section, Users can search Informative References based on a focal document of their choice. Users can also locate and retrieve an Informative Reference using a variety of fields, such as the type of Authority or Category of Submitter that an Informative Reference is cataloged as. Additionally, Users can perform keyword searches of catalog content and sort the catalog columns within the table in a variety of different ways.



Derived Relationship Mapping

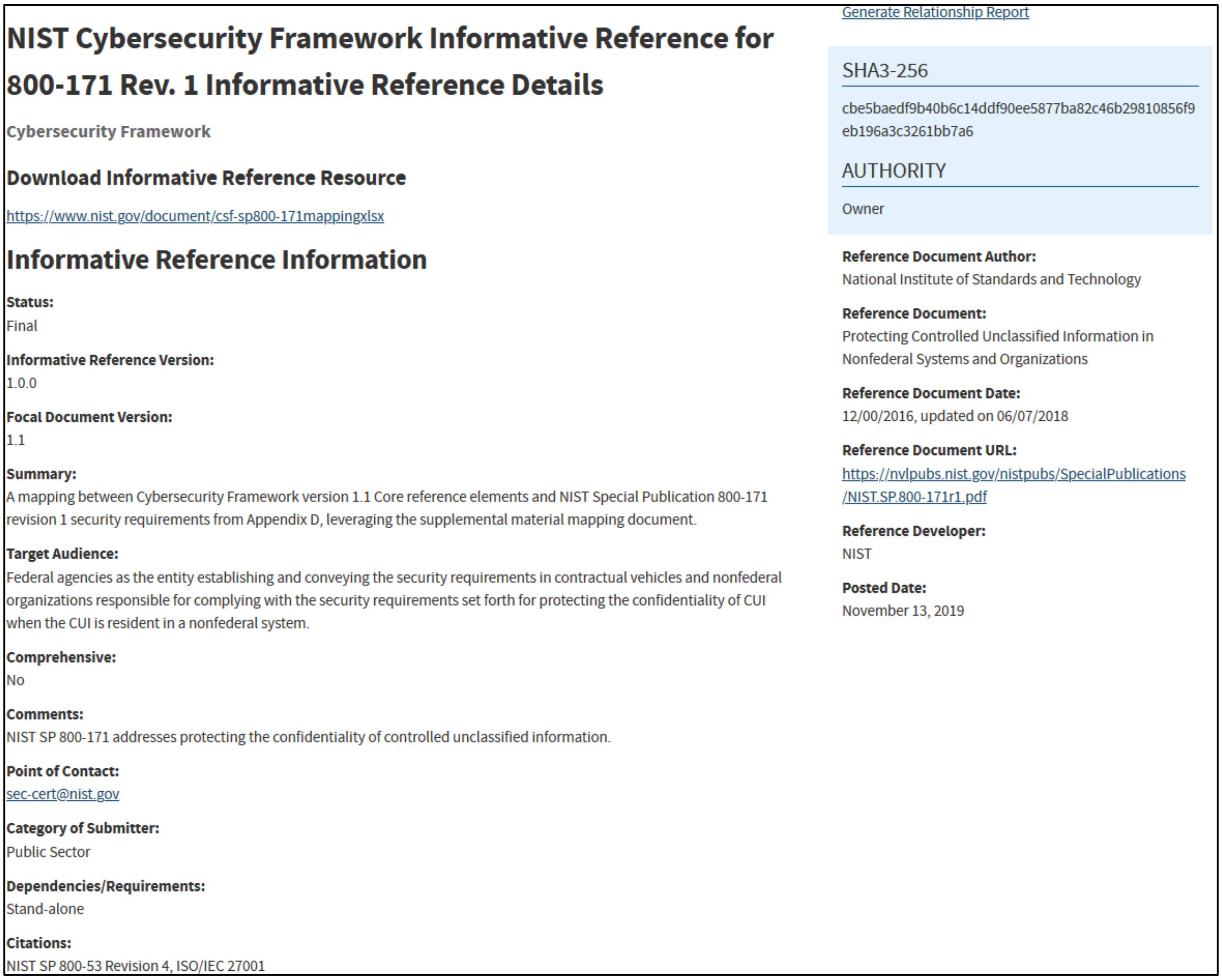
ADVANCED SEARCH

Focal Document	Cybersecurity Framework v1.1
Informative Reference Name	
Reference Document	
Posted Date	/ / to / /
Authority	□ Non-Owner □ Owner
Category of Submitter	□ Academia □ Other □ Private Sector □ Public Sector
Keyword(s)	
Sort By	Reference Document (A-Z)

Informative Reference (ver)	Reference Document	Posted Date	Focal Document	Submitting Organization	Authority	Category of Submitter
NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1 (1.0.0) (More Details)	NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management	05/19/20	Cybersecurity Framework v1.1	NIST	Owner	Public Sector

Figure 4: OLIR Catalog Page

Selecting the "More Details" link of an Informative Reference in the Catalog will display a description page, shown in Figure 5, that includes the General Information of an Informative Reference as provided by the Developer.



NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1 Informative Reference Details

Cybersecurity Framework

Download Informative Reference Resource

https://www.nist.gov/document/csf-sp800-171mappingxlsx

Informative Reference Information

Status:
Final

Informative Reference Version:
1.0.0

Focal Document Version:
1.1

Summary:
A mapping between Cybersecurity Framework version 1.1 Core reference elements and NIST Special Publication 800-171 revision 1 security requirements from Appendix D, leveraging the supplemental material mapping document.

Target Audience:
Federal agencies as the entity establishing and conveying the security requirements in contractual vehicles and nonfederal organizations responsible for complying with the security requirements set forth for protecting the confidentiality of CUI when the CUI is resident in a nonfederal system.

Comprehensive:
No

Comments:
NIST SP 800-171 addresses protecting the confidentiality of controlled unclassified information.

Point of Contact:
sec-cert@nist.gov

Category of Submitter:
Public Sector

Dependencies/Requirements:
Stand-alone

Citations:
NIST SP 800-53 Revision 4, ISO/IEC 27001

Generate Relationship Report

SHA3-256

cbe5baedf9b40b6c14ddf90ee5877ba82c46b29810856f9eb196a3c3261bb7a6

AUTHORITY

Owner

Reference Document Author:
National Institute of Standards and Technology

Reference Document:
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Reference Document Date:
12/00/2016, updated on 06/07/2018

Reference Document URL:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

Reference Developer:
NIST

Posted Date:
November 13, 2019

Figure 5: Informative Reference More Details Page

Table 2 lists fields and descriptions of the information depicted on the More Details page in Figure 5.

Table 2: Informative Reference More Details Description Fields

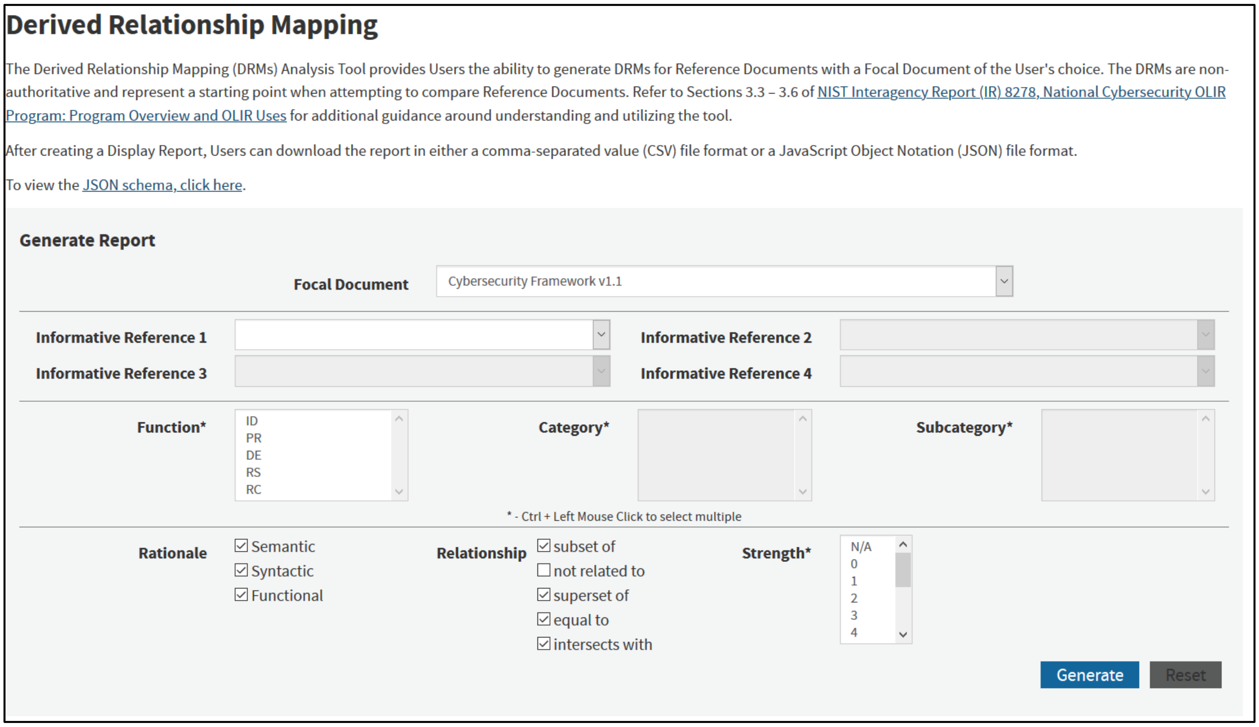
Field Name	Description
Informative Reference Name	The name by which the Informative Reference listing will be known. The format is a human-readable string of characters.
Focal Document	A source document that is used as the basis for comparing a concept with a concept from another document. As of this writing, the OLIR Program has three Focal Documents: the Cybersecurity Framework, the Privacy Framework, and SP 800-53 Rev. 4.
Web Address	The URL where the Informative Reference can be found
Status	Indicates if an Informative Reference is in “Draft” (not yet final) or “Final” (after the comments from the public comment period have been addressed)

Field Name	Description
Informative Reference Version	The version of the Informative Reference 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 Informative Reference. NIST recommends that Developers begin with the latest Focal Document version.[2]
Summary	The purpose of the Informative Reference
Target Audience	The intended audience for the Informative Reference
Comprehensive	Whether the Informative Reference 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 phone number within the Informative Reference Developer organization
Category of Submitter	The category type of the Informative Reference: • 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 and the products, services, or information covers topics related to the Focal Document • Academia: informative references which originate from educational institutions. Examples include universities, colleges, and research laboratories. • Other: informative references which do not fall into the previous categories are assigned the designation of "other." Examples include standards development organizations and international governments.
Dependencies/Requirements	Whether the Informative Reference is used in conjunction with other Informative Reference(s) or as a standalone Informative Reference
Citations	A listing of source material (beyond the Reference Document) that supported development of the Informative Reference
SHA3-256	The hash value checksum that is generated between the validated Informative Reference sent to the OLIR Program and the publicly available Informative Reference. The value is monitored to maintain data integrity of the Informative Reference.
Authority	The organization responsible for authoring the Informative Reference in relation to the organization that produced the Reference Document represented by the Informative Reference 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
Reference Developer	The organization(s) that created the Informative Reference
Posted Date	The date that a validated Informative Reference 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

[2] This field will be modified as additional Focal Documents are added to the OLIR Program.

3.3 The DRM Analysis Tool

The DRM Analysis Tool[3] provides Users with the ability to generate DRMs for Reference Documents with a Focal Document of the User's choice. The DRMs are non-authoritative and represent a starting point when attempting to compare Reference Documents. Figure 6 depicts the homepage of the DRM Analysis Tool.



Derived Relationship Mapping

The Derived Relationship Mapping (DRMs) Analysis Tool provides Users the ability to generate DRMs for Reference Documents with a Focal Document of the User's choice. The DRMs are non-authoritative and represent a starting point when attempting to compare Reference Documents. Refer to Sections 3.3 – 3.6 of NIST Interagency Report (IR) 8278, National Cybersecurity OLIR Program: Program Overview and OLIR Uses for additional guidance around understanding and utilizing the tool.

After creating a Display Report, Users can download the report in either a comma-separated value (CSV) file format or a JavaScript Object Notation (JSON) file format.

To view the JSON schema, click here.

Generate Report

Focal Document: Cybersecurity Framework v1.1

Informative Reference 1

Informative Reference 2

Informative Reference 3

Informative Reference 4

Function*: ID, PR, DE, RS, RC

Category*

Subcategory*

* - Ctrl + Left Mouse Click to select multiple

Rationale: ☑ Semantic ☑ Syntactic ☑ Functional

Relationship: ☑ subset of □ not related to ☑ superset of ☑ equal to ☑ intersects with

Strength*: N/A, 0, 1, 2, 3, 4

Figure 6: DRM Analysis Tool Home Page

As Figure 6 shows, when accessing the DRM Analysis tool, Users must first select the Focal Document for comparative analysis. Users have the ability to display potential relationships of up to four Informative References at a time for a given Focal Document. Users can generate reports at any level (i.e., Function, Category, Subcategory) of the Cybersecurity Framework or Control Family, Security/Privacy Control, or Security Control Enhancements for the SP 800-53 Rev. 4 Focal Document. When a User accesses this page, all rationale and relationships pairings (except for the "not related to" relationship) are pre-selected by default. To filter out any rationale or relationship selections, the User can deselect a checkbox as appropriate before generating a report.

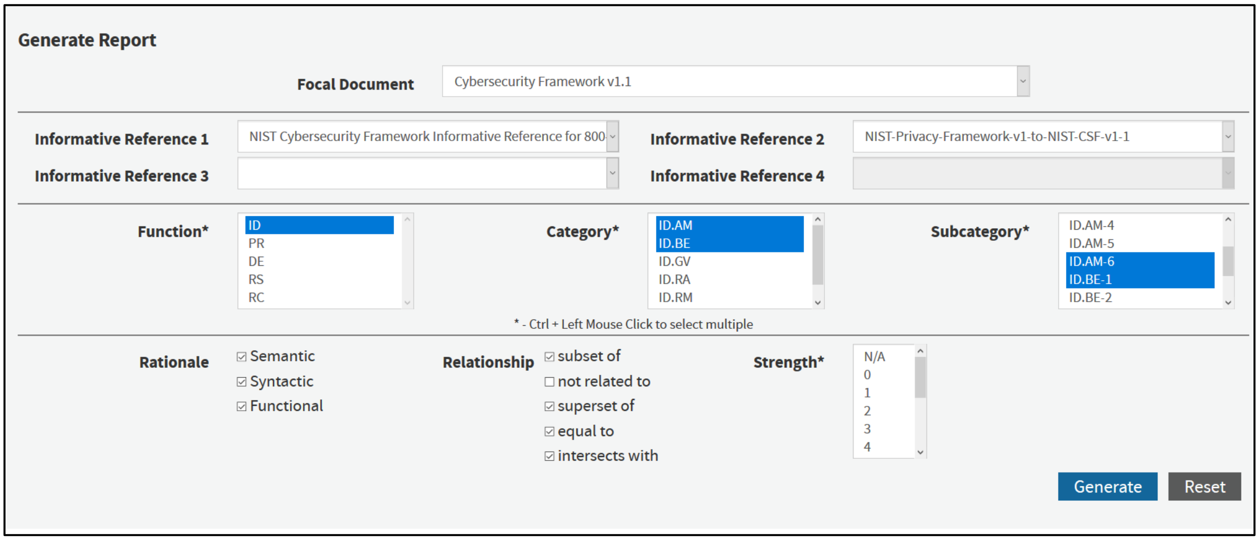
By default, the Strength of Relationship field is left unselected. Users can generate reports with this field unselected to display every type of strength defined within the Informative Reference

[3] See https://csrc.nist.gov/projects/cybersecurity-framework/derived-relationship-mapping.

of their search criteria. Users can narrow their criteria by selecting a singular or multiple strength pairing for further analysis.

In addition to performing an analysis at an individual level (i.e., selecting one Function, Category, or Subcategory), Users also have the ability to display Informative References at multiple levels (i.e., selecting multiple Functions, Categories, and Subcategories or multiple Control Families, Security/Privacy Controls, or Security Control Enhancements). Figure 7 displays an example of multiple Categories and Subcategories selected for User analysis when a User has selected the Cybersecurity Framework Focal Document. In this example, the two Categories being displayed are ID.AM and ID.BE along with Subcategories ID.AM-6 and ID.BE-1. The Strength of Relationship field has been left unselected.

To achieve this desired output, a User should first select the "Cybersecurity Framework v1.1" Focal Document from the drop-down menu. The User should then choose the Informative References for comparative analysis. Next, the User should select the 'ID' Function, which will result in the applicable Categories being displayed in the Category box. To select multiple Categories on a Windows computer, the user can hold the "Ctrl" key and click on the ID.AM and ID.BE Categories. On a macOS computer, the user can hold the "Command" key instead of the "Control" key. Choosing both ID.AM and ID.BE will cause all of the Subcategories within ID.AM and ID.BE to be displayed in the Subcategory box. Users can continue this selection behavior to select multiple Subcategories.



Generate Report

Focal Document: Cybersecurity Framework v1.1

Informative Reference 1: NIST Cybersecurity Framework Informative Reference for 800

Informative Reference 2: NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1

Informative Reference 3:

Informative Reference 4:

Function*: ID, PR, DE, RS, RC

Category*: ID.AM, ID.BE, ID.GV, ID.RA, ID.RM

Subcategory*: ID.AM-4, ID.AM-5, ID.AM-6, ID.BE-1, ID.BE-2

* - Ctrl + Left Mouse Click to select multiple

Rationale: ☑ Semantic ☑ Syntactic ☑ Functional

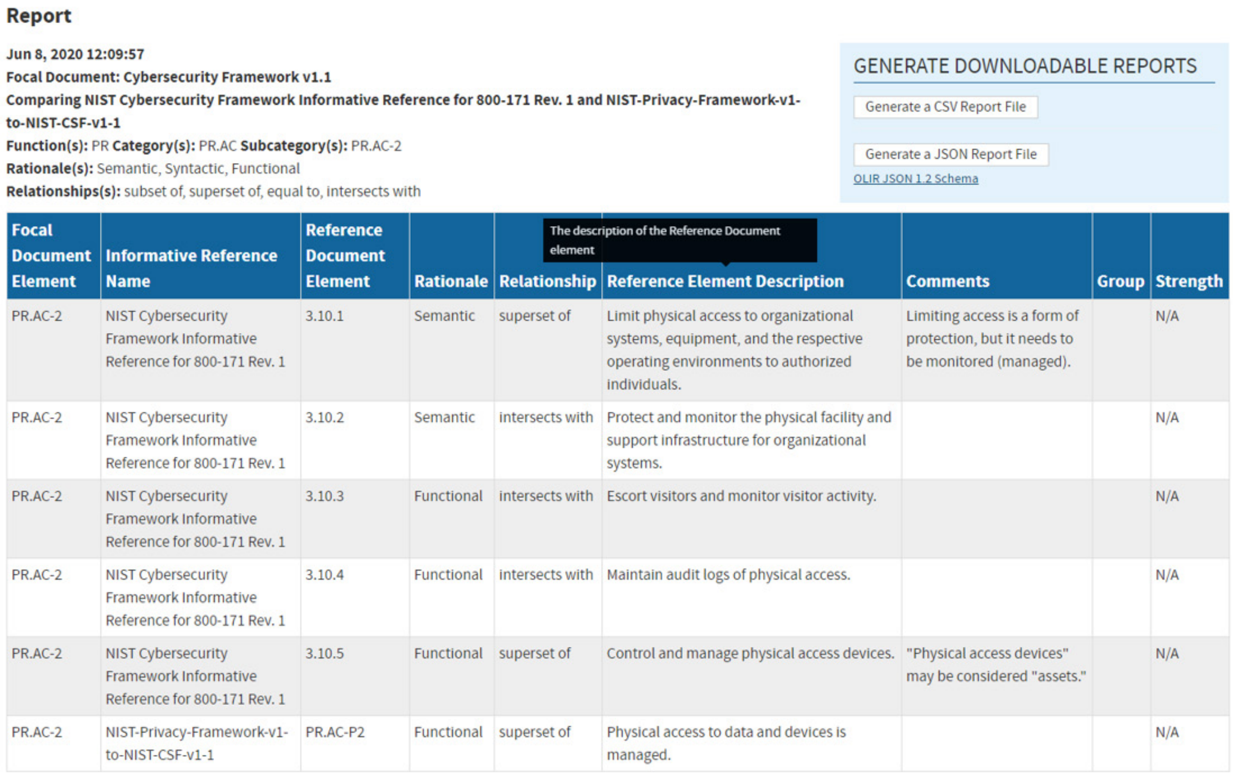
Relationship: ☑ subset of □ not related to ☑ superset of ☑ equal to ☑ intersects with

Strength*: N/A, 0, 1, 2, 3, 4

Figure 7: Multi-Select Example

3.4 Display Report

After selecting the 'Generate' option (see Figure 7), Users are presented with an on-screen output table. Figure 8 shows the results of comparing two Informative References at the individual PR.AC-2 Subcategory level with the Cybersecurity Framework Focal Document selected. This on-screen output is the *Display Report*.


GENERATE DOWNLOADABLE REPORTS
Generate a CSV Report File
Generate a JSON Report File
OLIR JSON 1.2 Schema
The description of the Reference Document element

Report

Jun 8, 2020 12:09:57
Focal Document: Cybersecurity Framework v1.1
Comparing NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1 and NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1
Function(s): PR **Category(s):** PR.AC **Subcategory(s):** PR.AC-2
Rationale(s): Semantic, Syntactic, Functional
Relationships(s): subset of, superset of, equal to, intersects with

Focal Document Element	Informative Reference Name	Reference Document Element	Rationale	Relationship	Reference Element Description	Comments	Group	Strength
PR.AC-2	NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1	3.10.1	Semantic	superset of	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	Limiting access is a form of protection, but it needs to be monitored (managed).		N/A
PR.AC-2	NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1	3.10.2	Semantic	intersects with	Protect and monitor the physical facility and support infrastructure for organizational systems.			N/A
PR.AC-2	NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1	3.10.3	Functional	intersects with	Escort visitors and monitor visitor activity.			N/A
PR.AC-2	NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1	3.10.4	Functional	intersects with	Maintain audit logs of physical access.			N/A
PR.AC-2	NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1	3.10.5	Functional	superset of	Control and manage physical access devices.	"Physical access devices" may be considered "assets."		N/A
PR.AC-2	NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1	PR.AC-P2	Functional	superset of	Physical access to data and devices is managed.			N/A

Figure 8: Display Report Example

Understanding Section 3.1.2 of this document is a prerequisite to understanding the Display Report. Due to screen space limitations, the Display Report stacks the results according to the Focal Document element. For example, if Reference A has two relationship pairings to a given Focal Document element, and Reference B has two relationship pairings to the same Focal Document element, the two Reference A relationships will be displayed in rows 1 and 2, followed by Reference B's relationships in rows 3 and 4, with the Focal Document element identifier in the leftmost column of all four rows.

Hover-over 'Tool Tips' are provided with descriptions when the User scrolls the pointer over the column headers. Figure 8 shows an example of a Tool Tip when a User hovers above the "Reference Element Description" column header. Likewise, the Cybersecurity Framework Core definitions are displayed using the same Tool Tips behavior when a User hovers over the Focal Document Element identifier displayed in the leftmost column.

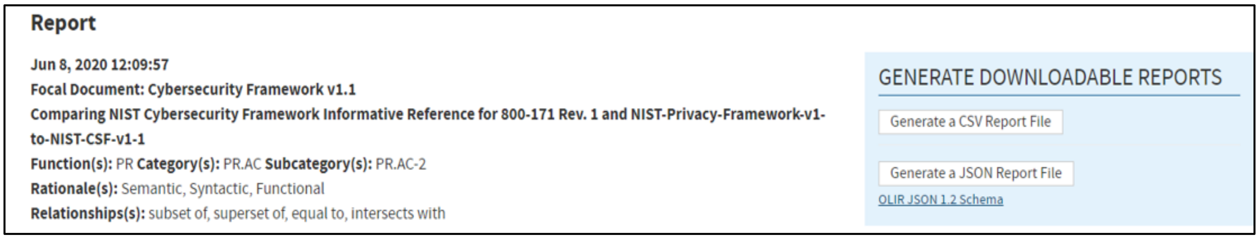
Table 3 provides a detailed description of the Display Report column headers.

Table 3: Display Report Column Header Descriptions

Field Name	Description
Focal Document Element	The identifier of the Focal Document element being mapped
Informative Reference Name	The name by which the Informative Reference listing will be referred
Reference Document Element	The identifier of the Reference Document element being mapped
Rationale	The explanation of why a Reference Document element and a Focal Document element are related. This will be one of the following: Syntactic, Semantic, or Functional.
Relationship	The type of logical relationship that the Reference Document Developer asserts compared to the Focal Document. The Developer conducting the assertion should focus on the perceived intent of each of the Reference and Focal Document elements. This will be one of the following, as depicted in Figure 1 (where “f” is a Focal Document element and “r” is a Reference Document element): Subset of, Intersects with, Equal to, Superset of, or Not related to.
Reference Element Description	The description of the Reference Document element
Comments	Notes to NIST or implementers
Group	The designation given to a Reference Document element when it is part of a group of Reference Document elements that correlates to a Focal Document element
Strength of Relationship	The extent to which a Reference Document element and a Focal Document element are similar

3.5 Report Downloads

After creating a Display Report, multiple report download options are available, as depicted in the right corner of Figure 9. Within “Generate Downloadable Reports” are links for a CSV (comma-separated values) report file and a JSON (JavaScript Object Notation) report file.[4] Clicking on a “Generate” link causes the corresponding report file format to be downloaded.



Report

Jun 8, 2020 12:09:57
Focal Document: Cybersecurity Framework v1.1
Comparing NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1 and NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1
Function(s): PR **Category(s):** PR.AC **Subcategory(s):** PR.AC-2
Rationale(s): Semantic, Syntactic, Functional
Relationships(s): subset of, superset of, equal to, intersects with

GENERATE DOWNLOADABLE REPORTS
Generate a CSV Report File
Generate a JSON Report File
OLIR JSON 1.2 Schema

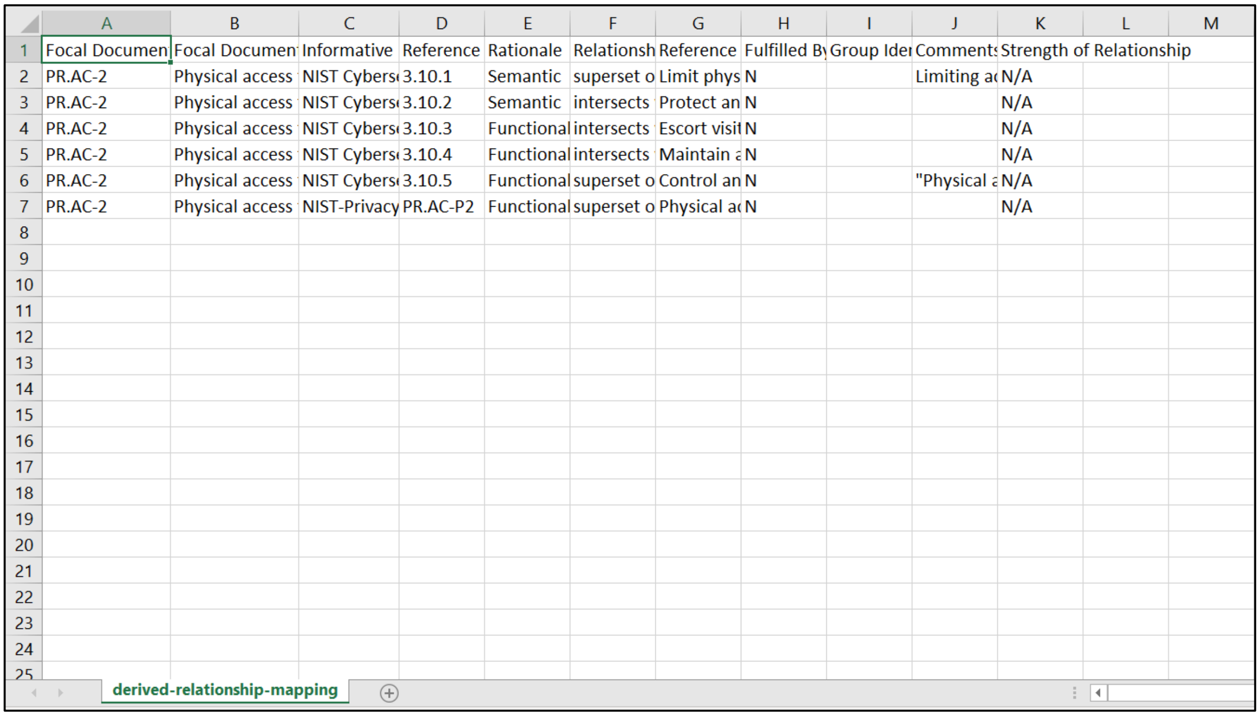
Figure 9: Report Download Options

[4] The CSV and JSON download links only become available after the Display Report is generated.

The report downloads contain more information than the Display Report (for example, Focal Document Element description) for more convenient human comparison and automated processing.[5]

3.5.1 Report Download in CSV Format

The CSV format 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 DRM Analysis Tool. Figure 10 represents a sample CSV report. The CSV file is consistent with the columns of the OLIR Informative Reference Focal Document template used by Reference Developers in NISTIR 8278A [2].



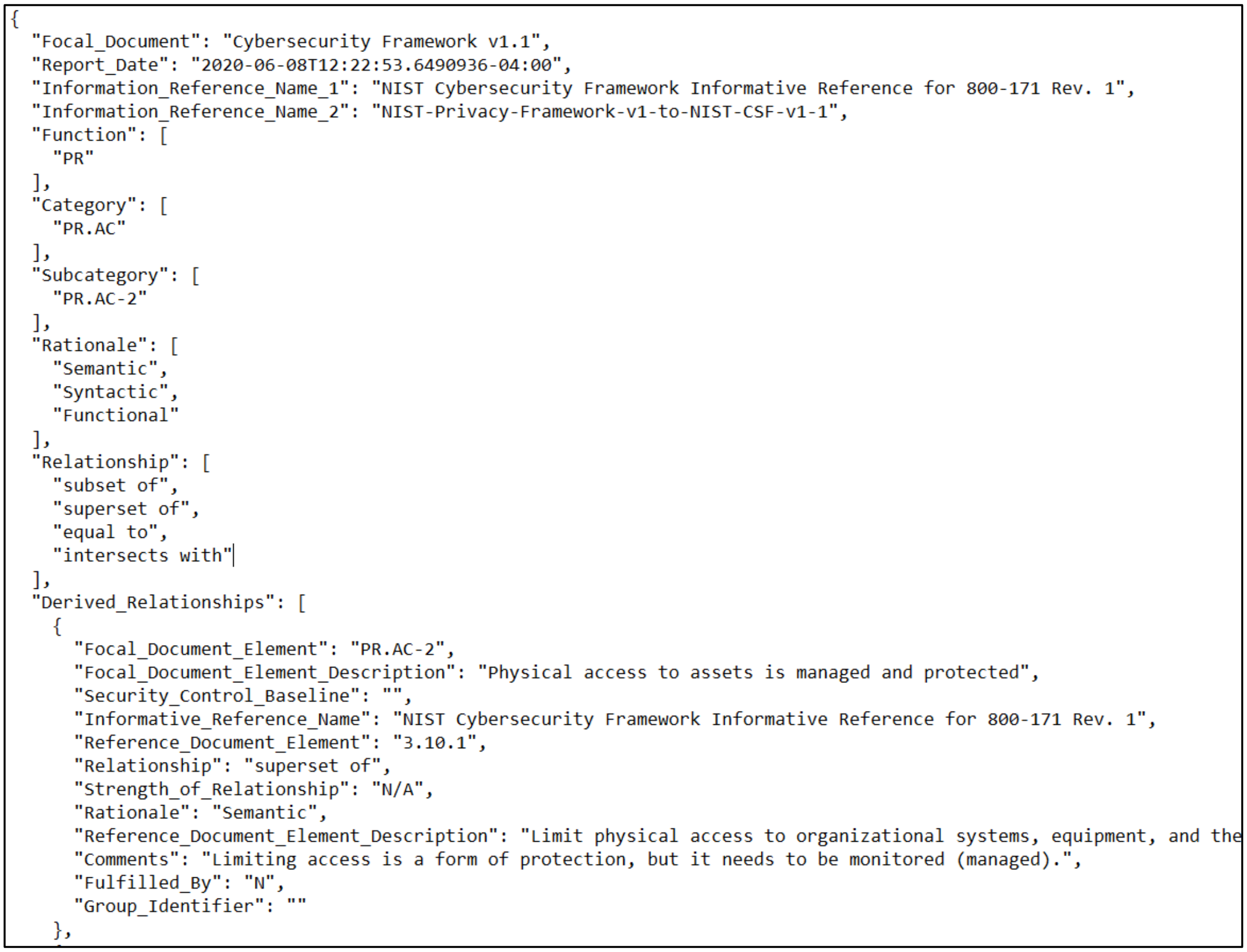
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Focal Documen	Focal Documen	Informative	Reference	Rationale	Relationsh	Reference	Fulfilled By	Group Ider	Comments	Strength of Relationship		
2	PR.AC-2	Physical access	NIST Cybers	3.10.1	Semantic	superset o	Limit phys	N		Limiting ac	N/A		
3	PR.AC-2	Physical access	NIST Cybers	3.10.2	Semantic	intersects	Protect an	N			N/A		
4	PR.AC-2	Physical access	NIST Cybers	3.10.3	Functional	intersects	Escort visit	N			N/A		
5	PR.AC-2	Physical access	NIST Cybers	3.10.4	Functional	intersects	Maintain a	N			N/A		
6	PR.AC-2	Physical access	NIST Cybers	3.10.5	Functional	superset o	Control an	N		"Physical a	N/A		
7	PR.AC-2	Physical access	NIST-Privacy	PR.AC-P2	Functional	superset o	Physical ac	N			N/A		

Figure 10: Sample CSV Report

3.5.2 Report Download in JSON Format

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 DRM Analysis Tool. The JSON file depicted in Figure 11 shows how the data is displayed. The JSON's file contents are consistent with the columns of the OLIR Informative Reference Focal Document template used by Reference Developers in NISTIR 8278A [2].

[5] See NISTIR 8278A [2] for additional field descriptions.



```
{
  "Focal_Document": "Cybersecurity Framework v1.1",
  "Report_Date": "2020-06-08T12:22:53.6490936-04:00",
  "Information_Reference_Name_1": "NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1",
  "Information_Reference_Name_2": "NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1",
  "Function": [
    "PR"
  ],
  "Category": [
    "PR.AC"
  ],
  "Subcategory": [
    "PR.AC-2"
  ],
  "Rationale": [
    "Semantic",
    "Syntactic",
    "Functional"
  ],
  "Relationship": [
    "subset of",
    "superset of",
    "equal to",
    "intersects with"
  ],
  "Derived_Relationships": [
    {
      "Focal_Document_Element": "PR.AC-2",
      "Focal_Document_Element_Description": "Physical access to assets is managed and protected",
      "Security_Control_Baseline": "",
      "Informative_Reference_Name": "NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1",
      "Reference_Document_Element": "3.10.1",
      "Relationship": "superset of",
      "Strength_of_Relationship": "N/A",
      "Rationale": "Semantic",
      "Reference_Document_Element_Description": "Limit physical access to organizational systems, equipment, and the
      "Comments": "Limiting access is a form of protection, but it needs to be monitored (managed).",
      "Fulfilled_By": "N",
      "Group_Identifier": ""
    },
```

Figure 11: Sample JSON Report

3.6 Common Use Cases

The DRM Analysis Tool output displays authoritative relationships. When a User compares the relationships from different Reference Documents and infers additional relationships among them, those inferred—*derived*—relationships are non-authoritative. However, they are still useful for a variety of use cases, and one such group is discussed in the following subsection. Additional use cases will be added to a subsequent version of this document.

3.6.1 Comparative Analysis of Cybersecurity Documents and Controls

Users often need to compare two cybersecurity or privacy documents for a variety of reasons, such as demonstrating where the documents' cybersecurity controls are similar and where gaps exist. This is true for cybersecurity or privacy document authors, auditors, and control implementers alike.

3.6.1.1 Without OLIR DRM

Before the OLIR Program, a person analyzing documents was often forced to conduct a manual comparison, typically by copying the contents of both documents into a spreadsheet for easier searching and sorting. The analyst 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 an analyst were comparing the Cybersecurity Framework with NIST SP 800-171 [7], they would start within the Cybersecurity Framework Reference Document at the "Asset Management (ID.AM) Category," 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, the analyst might select Section 3.4, "Configuration Management," of SP 800-171 and read through each of its basic and derived security requirements to identify relationships.

To save time, an analyst might try to leverage existing document mappings from SMEs. In this example, the analyst could leverage the mappings within SP 800-171 to SP 800-53 [6] controls, as well as the NIST Cybersecurity Framework, which contains mappings from its elements to SP 800-53 controls. So, SP 800-53 could 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 searching the Cybersecurity Framework Core for mappings to CM-8, it is determined that there is a relationship listed for subcategories ID.AM-1, ID.AM-2, PR.DS-3, and DE.CM-7. The analyst could then focus their comparative analysis on these controls.

This process would be repeated for all of the categories and subcategories within the Cybersecurity Framework and the basic and derived requirements of SP 800-171. Multiply this process by hundreds of analysts performing the same brute force process, and two problems quickly emerge: 1) the different opinions of analysts result in inconsistent associations, and 2) the analysts duplicate an enormous amount of effort. Streamlining this process is the main reason that the OLIR DRM capability was created.

3.6.1.2 With OLIR DRM

Since OLIR Catalog entries must comply with NISTIR 8278A [2], OLIR submissions are already decomposed and associated with a Focal Document (in this case, the NIST Cybersecurity Framework) using standard identifiers created by the document submitters. The stacked Display Report and report download options provide Users with a convenient way to quickly view how one document may relate to another by leveraging the Focal Document. The DRM Analysis Tool automates the brute force comparison method for comparing Reference Documents, rendering transitive relationship possibilities for the analyst to consider. Even though the stacked reference comparison is not authoritative since it is derived from inferences from authoritative first-order SME statements, it represents a good starting point for various types of comparative analysis and research.

With much of the relationship data defined by the SME (OLIR Developer) already, a User can simply generate a full report between two Reference Documents—selecting all desired Rationale and Relationship types and then exporting the stacked 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, a User 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.) Then, using the Rationale and Relationship designations, the User can better understand the similarities and differences between the elements and determine which relationships are relevant for their purposes.

To narrow down the potential for identifying strong associations between Reference Documents, a User could generate a Display Report using the Rationale and Relationship selectors to indicate association strength. By selecting options such as “Semantic” and “Equal to,” a User can parse the Display 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 an analyst knows that their organization already implements the NIST Privacy Framework, and NIST publishes a new version of SP 800-171, the analyst can generate a Display Report selecting the “Not related to” Relationship option. This report may contain data that is not relatable 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.
- An analyst could generate Display Reports in order to identify significant changes between two versions of the same document. First, the analyst could report on the relationships between the Privacy Framework and the current version of SP 800-171. Next, the analyst could report on the relationships between the Privacy Framework and a new draft revision of SP 800-171. Finally, the analyst could use a tool to compare those two reports and identify their differences.
- An analyst could identify the gaps that would need to be addressed if their organization adopted a new security framework by generating a Display Report comparing the Reference Documents they already comply 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 Display Report that shows which requirements from Reference Documents their products and services help to address. This provides a starting point for an analyst, who will need to do additional analysis for each identified requirement to determine the strength of each relationship.

In summary, the benefits to the User include faster analysis, the ability to leverage expert assertions, more structure in the analysis process, and better insight into the logic of the OLIR Developer.

References

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

[2] Barrett MP, Keller N, Quinn SD, Smith MC (2020) National Cybersecurity Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8278A. https://doi.org/10.6028/NIST.IR.8278A-draft

[3] Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. (The White House, Washington, DC), DCPD-201300091, February 12, 2013. https://www.govinfo.gov/app/details/DCPD-201300091

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

[5] 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.01162020

[6] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[7] 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

Appendix A—Acronyms

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

CSV	Comma-Separated Values
DRM	Derived Relationship Mapping
EO	Executive Order
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
IR	Interagency or Internal Report
ITL	Information Technology Laboratory
JSON	JavaScript Object Notation
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
OLIR	Online Informative References
OMB	Office of Management and Budget
SME	Subject Matter Expert
SP	Special Publication
URL	Uniform Resource Locator
USG	United States Government

Appendix B—Glossary

Developer
See *Informative Reference Developer*.

Focal Document
A source document that is used as the basis for comparing an element with an element from another document. As of this writing, the OLIR Program has three Focal Documents: the Cybersecurity Framework version 1.1, the Privacy Framework version 1.0*,* and SP 800-53 Rev. 4.

Focal Document Element
Any number and combination of organizational concepts (e.g., Functions, Categories, Subcategories, Controls, Control Enhancements) of a Focal Document.

Informative Reference
A relationship between a Focal Document Element and a Reference Document Element.

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

Non-Owner
An Informative Reference produced by anyone who is NOT the owner of the Reference Document.

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

Online Informative Reference (OLIR)
An Informative Reference expressed in NISTIR 8278A-compliant format and shared by the OLIR Catalog.

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

Reference
See *Informative Reference*.

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

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

User
A person, team, or organization that accesses or otherwise uses an Online Informative Reference.