Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been followed by the document identified below.

Withdrawal Date February 26, 2024

Original Release Date December 8, 2022

The attached draft document is followed by:

Status Final

Series/Number NIST IR 8278r1

Title National Online Informative References (OLIR) Program: Overview, Benefits, and Use

Publication Date February 2024

DOI https://doi.org/10.6028/NIST.IR.8278r1

CSRC URL https://csrc.nist.gov/pubs/ir/8278/r1/final

Additional Information

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

NIST Internal Report
NIST IR 8278r1 ipd

National Online Informative References (OLIR) Program:

Overview, Benefits, and Use

Initial Public Draft

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.ipd

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

NIST Internal Report
NIST IR 8278r1 ipd

National Online Informative References (OLIR) Program:

Overview, Benefits, and Use

Initial Public Draft

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.ipd

December 2022

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 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 the National Institute of Standards and Technology (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.

How to Cite this NIST Technical Series Publication:
Keller N, Quinn S, Scarfone, K, Smith M, Johnson V (2022) National Online Informative References (OLIR) Program: Overview, Benefits, and Use. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8278r1 ipd. https://doi.org/10.6028/NIST.IR.8278r1.ipd

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

Public Comment Period
December 8, 2022 – January 20, 2023

Submit Comments
olir@nist.gov

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

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

Abstract

Information and communication 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 of specifying relationships that can be used by both humans and automation. The National OLIR Program is a NIST effort to encourage and facilitate subject matter experts in defining OLIRs 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

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

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.

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

Table of Contents

1 Introduction 1
1.1 Purpose and Scope 2
1.2 Document Structure 2
2 OLIR Overview 3
2.1 Understanding Relationships 4
2.1.1 Relationship Rationales 4
2.1.2 Relationship Types 5
2.1.3 Relationship Strength 8
2.2 Reference Data in the OLIR Catalog 9
2.2.1 OLIRs 9
2.2.2 Derived Relationship Mappings (DRMs) 10
2.3 NIST Cybersecurity and Privacy Reference Tool (CPRT) 12
3 Using the OLIR Catalog 13
3.1 Searching the OLIR Catalog 13
3.2 Using the DRM Analysis Tool 18
3.3 Generating a Display Report 19
3.4 Downloading a Report 21
3.5 Inferring Additional Relationships Between Reference Documents 23
References 25
Appendix A. List of Symbols, Abbreviations, and Acronyms 26
Appendix B. Glossary 27
Appendix C. Change Log 28

List of Tables

Table 1. Relationship Type Descriptions 5
Table 2. OLIR More Details Description Fields 14
Table 3. Display Report Column Header Descriptions 21

List of Figures

Fig. 1. Relationship Types 5
Fig. 2. Example of Subset Relationship 6
Fig. 3. Example of Intersects Relationship 6
Fig. 4. Example of Equal Relationship 7
Fig. 5. Example of Superset Relationship 7
Fig. 6. Example of Unrelated Concepts 8
Fig. 7. Relative Strength of Relationships 9
Fig. 8. Multiple Documents Related to a Focal Document 11
Fig. 9. OLIR More Details Page 14

Fig. 10. OLIR Catalog Page 17
Fig. 11. DRM Analysis Tool Home Page 18
Fig. 12. Multi-Select Example 19
Fig. 13. Display Report Example 20
Fig. 14. Report Download Options 21
Fig. 15. Sample CSV Report 22
Fig. 16. Sample JSON Report 22

1 Introduction

Information and communication 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 standards, guidelines, frameworks, and regulations it *must* follow as well as what it *chooses* to follow. Each of these documents has a unique set of requirements and recommendations, and each document creator typically organizes and presents 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 make sense of them as a whole. Here are some notional examples of what you might need to know:

- Implementing new security control X would help satisfy particular requirements and recommendations in four documents.
- You need to update your remote access policy to include a requirement from document A. That requirement is more stringent than what the other documents state, so updating the policy to include what document A needs should help address the corresponding items in 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 that you are subject to.

Knowing these things involves identifying the relationships between the items in the documents. Figuring that out yourself is usually time-consuming and prone to error, especially because you are unlikely to be an expert on the documents. Some documents include 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 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 *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 of one document relate to items of another document. However, within the context of this document and the National OLIR Program, a *mapping* indicates the relationships between elements (items) of 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).

An *Online Informative Reference (OLIR)* records the relationships between elements of two documents as either a crosswalk (a *crosswalk OLIR*) or a mapping (a *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 automation. Automated approaches are necessary because of the ever-expanding pool of documents. Defining OLIRs outside of 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 standard defined by NIST Interagency or 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 defining OLIRs and submitting 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 8278A [2] for expressing OLIRs in a standardized and consistent manner.

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

- Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) version 1.1 [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 facilitates third parties in defining OLIRs between 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 information and communications technology domain documents, including 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 between 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.

Each crosswalk OLIR indicates pairs of Focal Document Elements and Reference Document Elements that have relationships. Each mapping OLIR does that as well but also characterizes each element-to-element relationship by its rationale, type, completeness, and (optionally) strength. Each of these is discussed in the following subsections. People already implicitly identify these characteristics but are not aware of doing so. One of the goals of the National OLIR Program is to elucidate the science by encouraging explicit declarations of OLIR relationship characteristics.

2.1.1 Relationship Rationales

The basic reason why a Reference Document Element and a Focal Document Element are related is attributed to one of three *rationales*:

1. **Syntactic** – Compares the **linguistic meaning** of the two elements. For example, the following statements have the same syntax:

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

2. **Semantic** – Compares the **contextual meaning** of the two elements. For example, the following statements convey the same semantic meaning:

   “The 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.”

3. **Functional** – Compares the **functions** of the two elements. For example, the following statements have the same functional result:

   printf (“foo\n”); [... C programming language]
   print “foo” [... BASIC programming language]

Each of these examples has two statements that could be considered equal **within the scope of the rationale**. While the statements in the last example may be functionally equivalent, they are not semantically equivalent because they describe different ways to achieve the same functionality, and they are of course not syntactically equivalent because their wordings are

much different. Most relationships captured by OLIRs are not of equal or equivalent statements. The next subsection examines this in more detail.

2.1.2 Relationship Types

Each relationship between a Focal Document Element and a Reference Document Element is classified by a *relationship type*. The relationship type indicates how the meanings of the two elements are related within the context of a particular rationale (e.g., syntactic, semantic, or functional). For each relationship, the relationship 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.

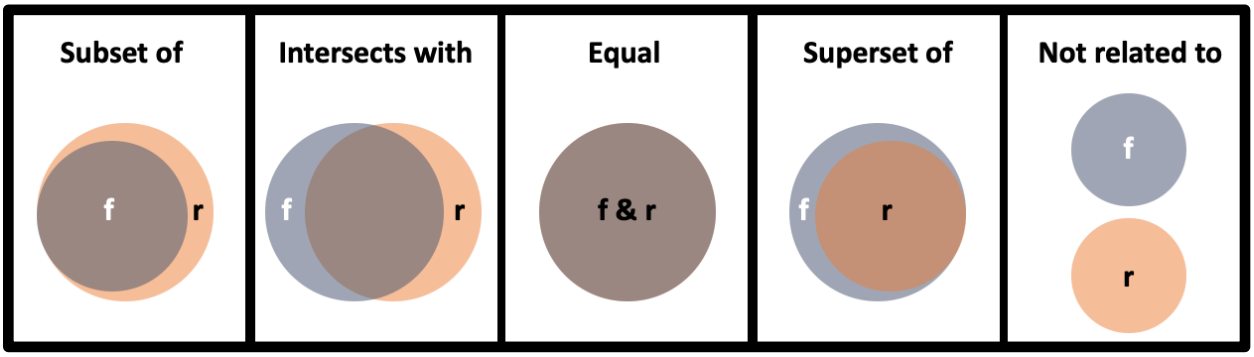


Fig. 1. Relationship Types

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 though 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.

Relationship types have a natural order: Equal, Subset and Superset, Intersects with, and Not Related. The Equal type indicates the most in common between the elements, and Not Related assertions indicate nothing in common.

The examples below illustrate each of the five relationship types. The Reference Document Elements are from NIST SP 800-171, and the Focal Document Elements are from version 1.1 of the Cybersecurity Framework.

Example 1: Subset

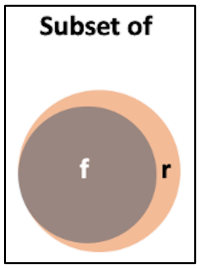


Fig. 2. Example of Subset Relationship

- Focal Document Element: PR.AT-4, "Senior executives understand their roles and responsibilities."
- Reference Document Element: Requirement 3.2.2, "Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities."

The OLIR Developer selects the functional rationale for this relationship. PR.AT-4 states that a specific group of users (senior executives) should be trained on their roles and responsibilities. Requirement 3.2.2 states that "all users" should be trained on their roles and responsibilities. The Developer asserts that the concept "all users" contains the concept "senior executives and others."

Because PR.AT-4 is one part of requirement 3.2.2, and PR.AT-4 does not contain any concepts that requirement 3.2.2 does not contain, the relationship type is Subset. In other words, PR.AT-4 (the Focal Document Element) is a subset of requirement 3.2.2 (the Reference Document Element).

Example 2: Intersects with

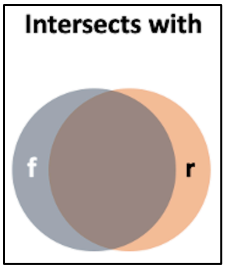


Fig. 3. Example of Intersects Relationship

- Focal Document Element: RS.CO-2, "Incidents are reported consistent with established criteria."
- Reference Document Element: Requirement 3.6.2, "Track, document, and report incidents to appropriate organizational officials and/or authorities."

The OLIR Developer selects the semantic rationale for this relationship. Both RS.CO-2 and requirement 3.6.2 address the same concept of documenting and reporting incidents. However, RS.CO-2 contains the concept of "established criteria," and requirement 3.6.2 contains the concept of "appropriate organizational officials and authorities."

Because the two elements address the same concept, but each element also includes an additional concept that the other does not include, the relationship type is Intersects with. In other words, RS.CO-2 (the Focal Document Element) intersects with requirement 3.6.2 (the Reference Document Element).

Example 3: Equal

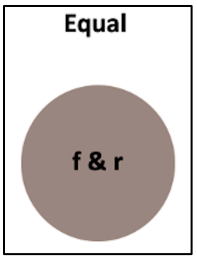


Fig. 4. Example of Equal Relationship

- Focal Document Element: PR.PT-3, "The principle of least functionality is incorporated by configuring systems to provide only essential capabilities."
- Reference Document Element: Requirement 3.4.6, "Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities."

The OLIR Developer could select either functional or semantic as the rationale for this relationship. Both PR.PT-3 and requirement 3.4.6 communicate the concept of "employing/incorporating the principle of least functionality by configuring systems to provide only essential capabilities." Neither PR.PT-3 nor requirement 3.4.6 contains any concepts that the other does not.

Because the two elements say the same thing, the relationship type is Equal. In other words, PR.PT-3 (the Focal Document Element) is equal to requirement 3.4.6 (the Reference Document Element).

Example 4: Superset of

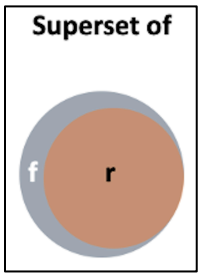


Fig. 5. Example of Superset Relationship

- Focal Document Element: PR.AC-1, "Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes."
- Reference Document Element: Requirement 3.5.1, "Identify system users, processes acting on behalf of users, and devices."

The Developer selects functional as the rationale for this relationship. PR.AC-1 includes several concepts for device, user, and process identities and credentials, including issuing, managing, verifying, revoking, and auditing them. Requirement 3.5.1 is about identifying devices, users, and processes, which is needed for PR.AC-1. However, requirement 3.5.1 does not include any of the other parts of PR.AC-1.

Because requirement 3.5.1 is one part of PR.AC-1, and requirement 3.5.1 does not contain any concepts that PR.AC-1 does not contain, the relationship type is Superset. In other words, PR.AC-1 (the Focal Document Element) is a superset of requirement 3.5.1 (the Reference Document Element).

Example 5: Not related to

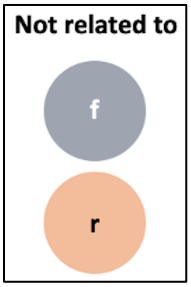


Fig. 6. Example of Unrelated Concepts

This relationship type is used when the Focal Document Element and the Reference Document Element do not share any concepts. In OLIRs submitted to the OLIR Catalog, Reference Document Elements that do not relate to any Focal Document Elements are either marked as "not related to" or omitted altogether.

2.1.3 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 7 illustrates how a single relationship type can encompass relationships of different strengths. For example, Case 1 shows a Focal Document Element and a Reference Document Element 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.

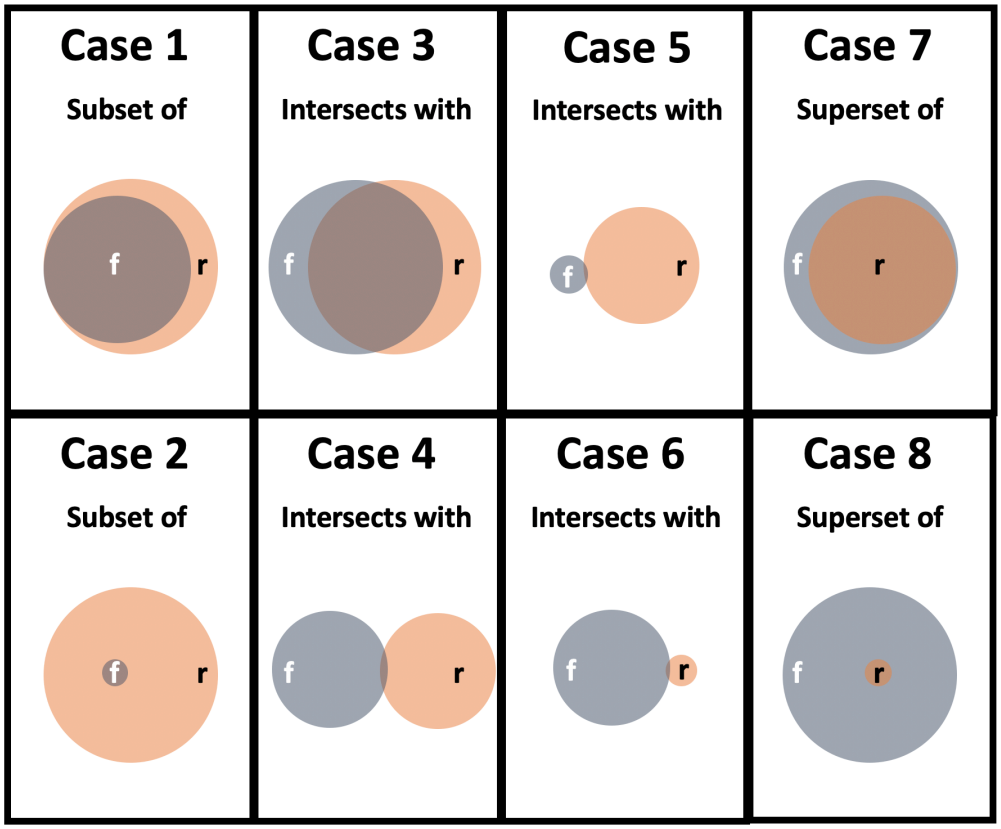


Fig. 7. Relative Strength of Relationships

The Program encourages OLIR Developers to include a measure 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."

2.2 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.

2.2.1 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.

2.2.2 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 Derived Relationship Mappings (DRM) tool. 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 DRM Analysis 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 8 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 Figure 8, 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.

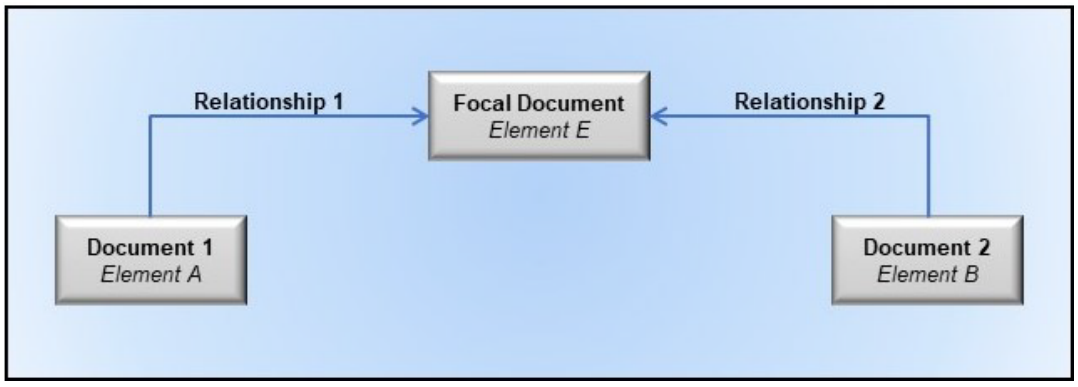


Fig. 8. Multiple Documents Related to a Focal Document

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 you want to compare Element PR.AC-1, "Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes" [1], to 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-1 is at a higher level than IA-7, which specifies, in detail, one part of what PR.AC-1 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 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, you 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. 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-1, ID.AM-2, PR.DS-3, and DE.CM-7. 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.

2.3 NIST Cybersecurity and Privacy Reference Tool (CPRT)

The NIST Cybersecurity and Privacy Reference Tool (CPRT) 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. These datasets, which include several of the OLIR Focal Documents, will make it much easier for users to identify, locate, compare, and customize content in and across NIST resources without needing to review hundreds of pages of narrative within the publications. The reference data can be exported in different data formats, including a machine-readable JavaScript Object Notation (JSON) format.

The CPRT project is in its initial phase as of this writing. 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 has 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 Figure 9, that includes the General Information of an OLIR.

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

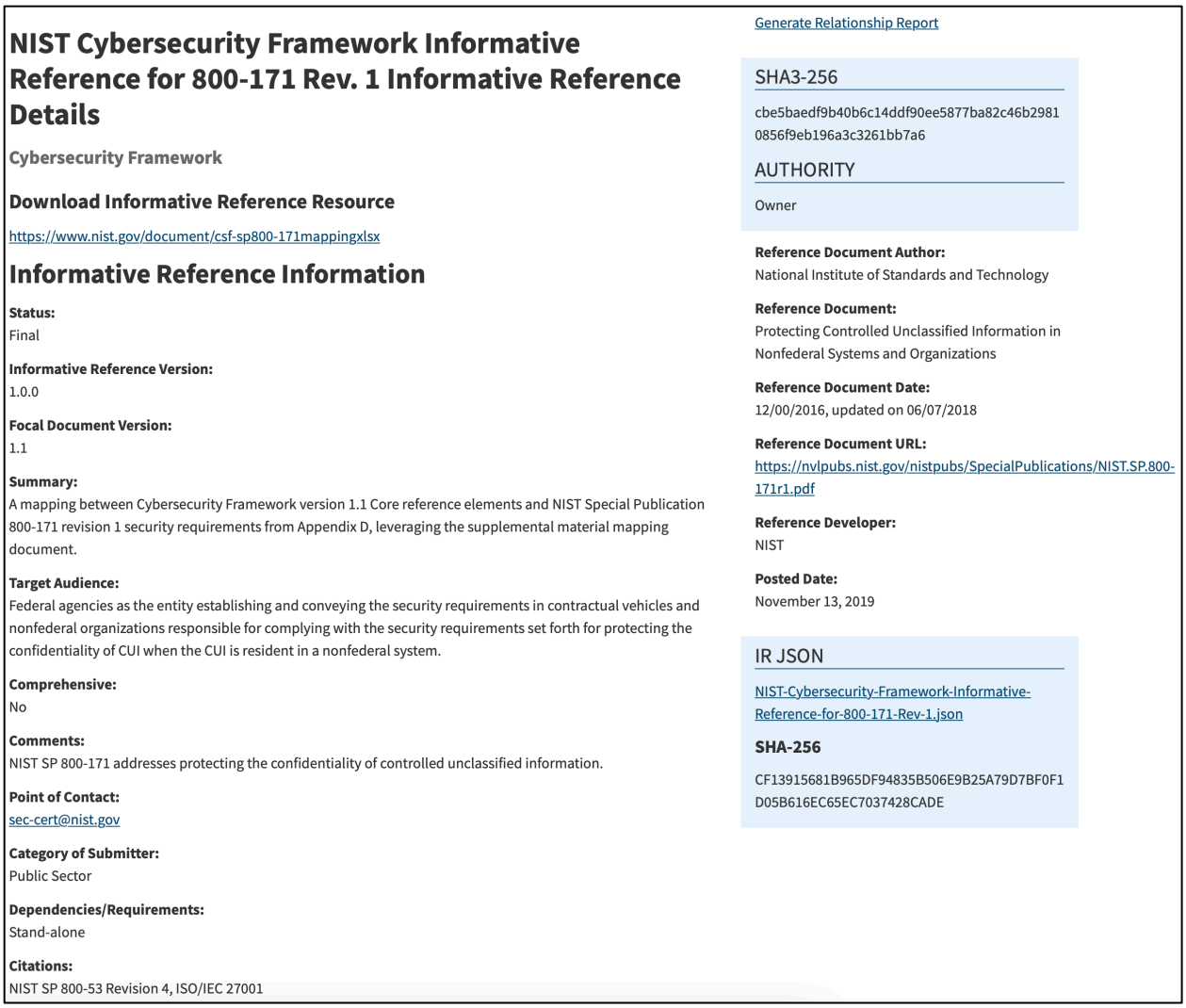


Fig. 9. OLIR More Details Page

Table 2 lists fields and descriptions of the information depicted on the More Details page in Figure 9.

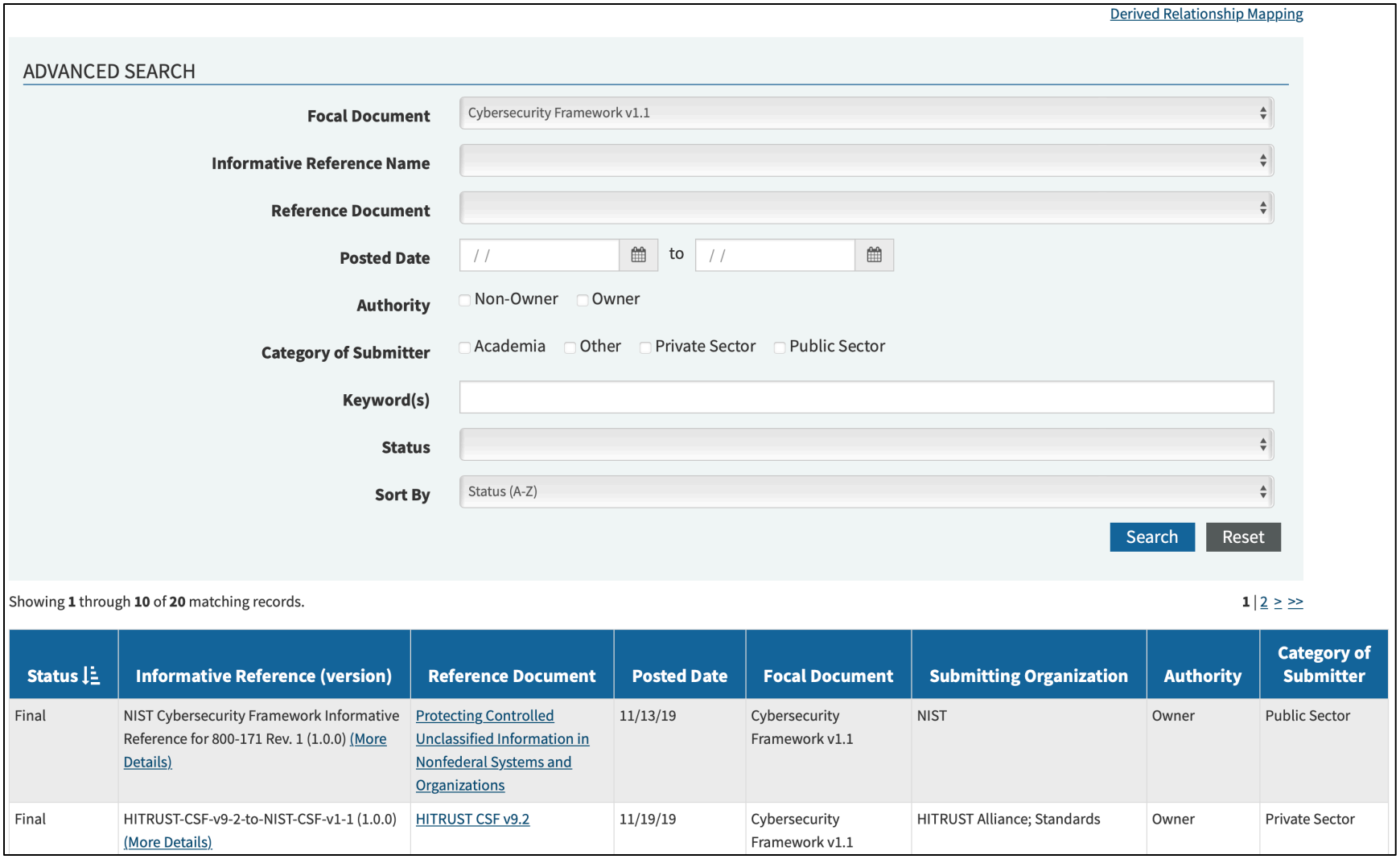
Table 2. OLIR More Details Description Fields

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 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
Reference Developer	The organization(s) that created the OLIR

Field Name	Description
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 10 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, and Submitting Organization. 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 cataloged as. Additionally, you can perform keyword searches of catalog content and sort the catalog columns within the table in a variety of different ways.



519 **Fig. 10.** OLIR Catalog Page

3.2 Using the DRM Analysis Tool

The DRM Analysis Tool[2] allows to generate DRMs for Reference Documents with a Focal Document of your choice. The DRMs are non-authoritative and represent a starting point when attempting to compare Reference Documents. Figure 11 depicts the homepage of the DRM Analysis Tool.

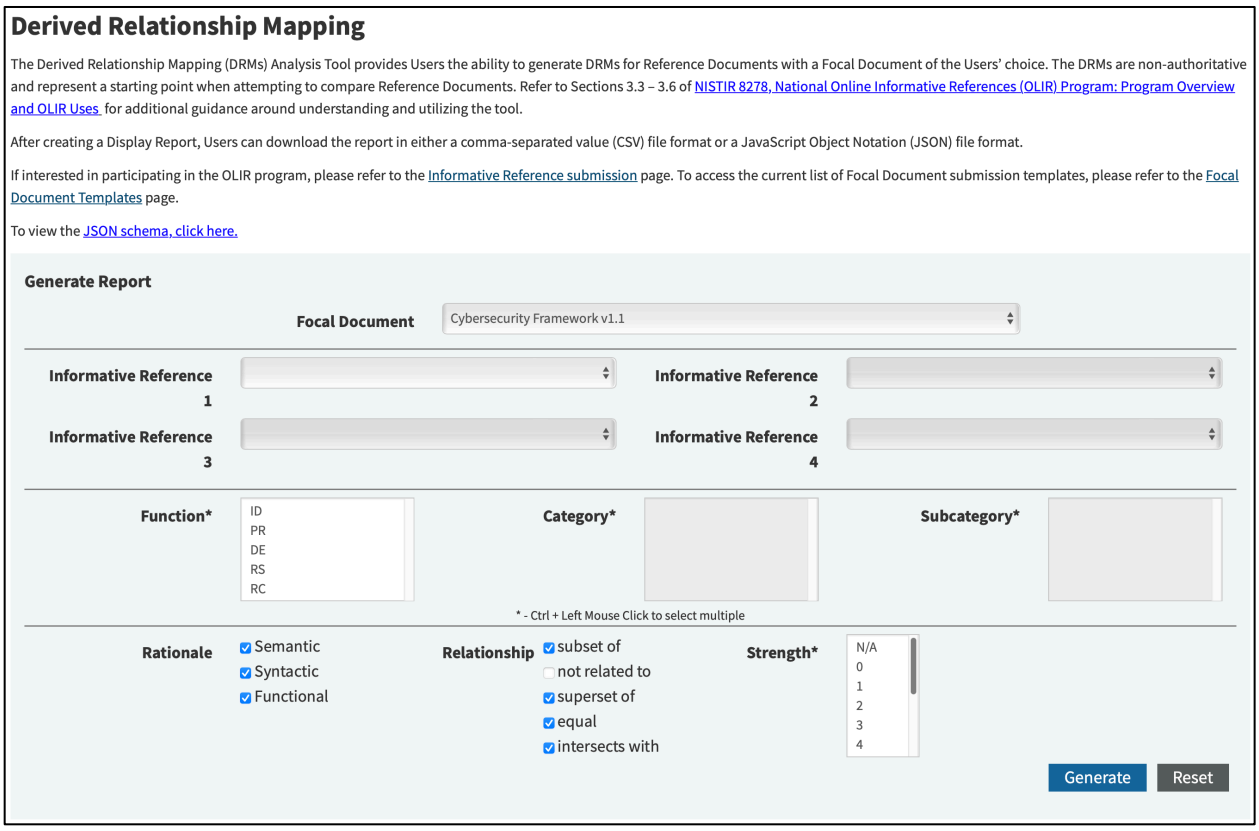


Fig. 11. DRM Analysis Tool Home Page

As Figure 11 shows, when accessing the DRM Analysis tool, you first select the Focal Document for comparative analysis. Only Focal Documents with two or more OLIRs in the OLIR Catalog are selectable in the Focal Document drop-down box. You can display potential relationships for up to four OLIRs at a time for a given Focal Document. For example, 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).

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

By default, the Strength of Relationship field is left unselected. You can generate reports with this field unselected to display every type of strength defined within the OLIR of their search

[2] See https://csrc.nist.gov/Projects/olir/derived-relationship-mapping.

criteria. You can narrow your 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), you can also display OLIRs at multiple levels (i.e., selecting multiple Functions, Categories, and Subcategories or multiple Control Families, Security/Privacy Controls, or Security Control Enhancements). Figure 12 displays an example of multiple Categories and Subcategories being selected for the Cybersecurity Framework Focal Document. In this example, the two displayed Categories 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, you should first select the "Cybersecurity Framework v1.1" Focal Document from the drop-down menu. Then choose the OLIRs for comparative analysis. Next, 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, you can hold the "Ctrl" key and click on the ID.AM and ID.BE Categories. On a macOS computer, you can hold the "Command" key instead. 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. You can continue this selection behavior to select multiple Subcategories.

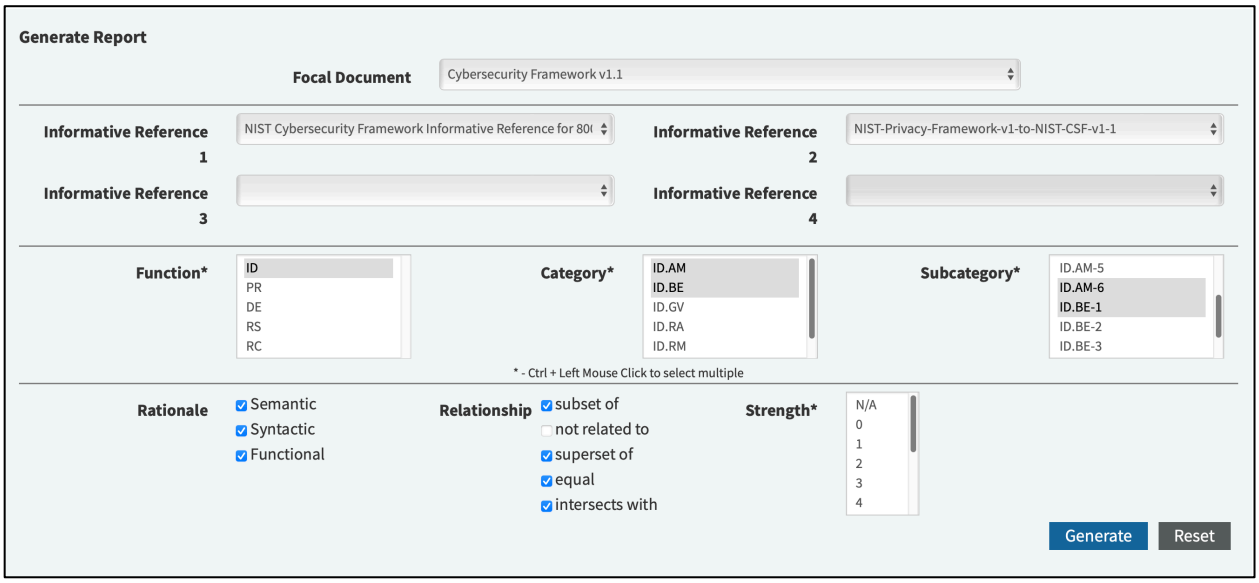


Fig. 12. Multi-Select Example

3.3 Generating a Display Report

After selecting the "Generate" option (see Figure 12), you are presented with an on-screen output table. Figure 13 shows the results of comparing two OLIRs at the individual PR.AC-2 Subcategory level with the Cybersecurity Framework Focal Document selected. This on-screen output is the *Display Report*.

Report

Jun 11, 2022 09:19:00
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, intersects with

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

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

Fig. 13. Display Report Example

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 you scroll the pointer over the column headers. Figure 13 shows an example of a Tool Tip when hovering above the "Reference Element Description" column header. 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.

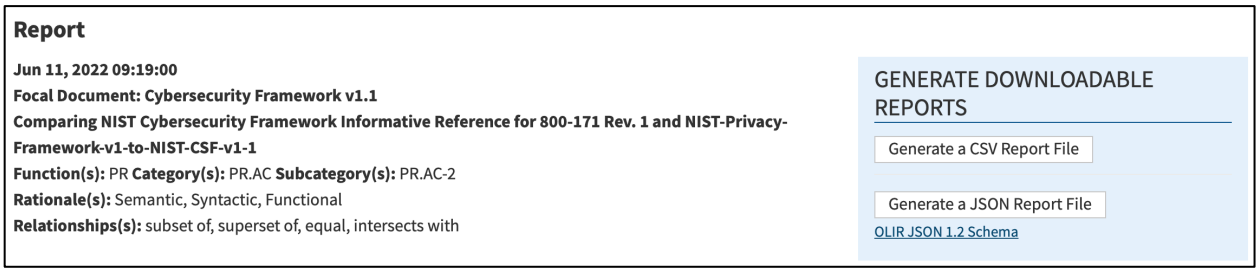
Table 3 provides a detailed description of the Display Report column headers.

577 **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 for why a Reference Document Element and a Focal Document Element are related. This will be syntactic, semantic, or functional.
Relationship	The type of logical relationship that the OLIR Developer asserts the Reference Document Element has compared to the Focal Document Element. The Developer conducting the assertion should focus on the perceived intent of each of the Elements. This will be one of the following, as depicted in Figure 1: 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. For example, SP 800-53 control AC-13 may have been split into three pieces so that relationships can be identified for each piece. Each piece would have its own row in the Display Report, a unique Focal Document Identifier (e.g., AC-13:1, AC-13:2, AC-13:3), and the same Group identifier (e.g., AC-13).
Strength of Relationship	The extent to which a Reference Document Element and a Focal Document Element are similar

578 ## 3.4 Downloading a Report

579 After creating a Display Report, multiple report download options are available, as depicted in
580 the right corner of Figure 14. Within "Generate Downloadable Reports" are links for CSV
581 (comma-separated values) and JSON report files.[3] Clicking on a "Generate" link causes the
582 corresponding report file format to be downloaded. The report downloads contain more
583 information than the Display Report (e.g., Focal Document Element description) for more
584 convenient human comparison and automated processing.[4]



585

586 **Fig. 14.** Report Download Options

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

Figure 15 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 DRM Analysis Tool.

	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 Iden	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		
8													

Fig. 15. 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 DRM Analysis Tool. The JSON file depicted in Figure 16 shows how the data is displayed.


```
{
  "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": ""
    },
```


Fig. 16. Sample JSON Report

3.5 Inferring Additional Relationships Between Reference Documents

The stacked Display 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 DRM Analysis Tool automates the brute force comparison method for analyzing Reference Documents and renders transitive relationship possibilities for the analyst to consider. The DRM Analysis 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 by selecting all desired Rationale and Relationship types and 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, 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.) Then, using the Rationale and Relationship designations, you can better understand the similarities and differences between the elements and determine which relationships are relevant.

To narrow the potential for identifying strong associations between Reference Documents, you could generate a Display Report using the Rationale and Relationship selectors to indicate association strength. By selecting options such as “semantic” and “equal to,” you 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 you know your organization already implements the NIST Privacy Framework, and NIST publishes a new version of SP 800-171, you can generate a Display Report selecting the “not related to” Relationship option. This report may contain data that is 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 Display 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 Display 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 Display 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 (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.6

[2] Barrett MP, Keller N, Quinn SD, Smith MC, Scarfone KA (2022) National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8278A. https://doi.org/10.6028/NIST.IR.8278Ar1.ipd

[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

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 Communication Technology

IoT
Internet of Things

IR
Interagency or 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

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

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 source 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 1.1, 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 of a Focal Document.

Informative Reference
See *Online Informative Reference*.

Informative Reference Developer
See *OLIR Developer*.

mapping OLIR
An OLIR that characterizes each relationship between pairs of elements, including the rationale for indicating the connection between the elements and the relationship type based on set theory principles.

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 two types of OLIRs: crosswalk and 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 of a Reference Document.

Appendix C. Change Log

In 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)