NISTIR 8278A

National Online Informative References (OLIR) Program:

Submission Guidance for OLIR Developers

Matthew Barrett
Nicole Keller
Stephen Quinn
Matthew C. Smith
Karen Scarfone

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

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

NISTIR 8278A

National Online Informative References (OLIR) Program:

Submission Guidance for OLIR Developers

Matthew Barrett*
Applied Cybersecurity Division
Information Technology Laboratory

Matthew C. Smith
Huntington Ingalls Industries
Annapolis Junction, MD

Nicole Keller
Stephen Quinn
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

**Former employee; all work for this publication was done while at NIST*

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

November 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 8278A
40 pages (November 2020)

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

Comments on this publication may be submitted to:

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

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 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, NIST Privacy Framework, and Special Publication 800-53. This document assists Informative Reference Developers (Developers) in understanding the processes and requirements for participating in the Program. The primary focus of the document is to instruct Developers on how to complete the OLIR Template spreadsheet when submitting an Informative Reference to NIST for inclusion in the OLIR Catalog. This document replaces Interagency or Internal Report (IR) 8204, *Cybersecurity Framework Online Informative References (OLIR) Submissions: Specification for Completing the OLIR Template*.

Keywords

crosswalk; Informative References; mapping; Online Informative References (OLIR).

Acknowledgments

The authors would like to thank all of those who commented on and contributed to this document.

Audience

The primary audience for this publication are individuals interested in developing Informative References for the National OLIR Program. The secondary audience are users who require additional details about the OLIRs posted in the OLIR Catalog.

Trademark Information

Document Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in Request for Comment (RFC) 2119 [1]. When these words appear in regular case, such as “should” or “may”, they are not intended to be interpreted as RFC 2119 key words.

Note to Readers

This specification is not meant to be read in sequential order. It is a reference for developers of OLIRs to provide clarity and direction when creating an OLIR. Developers are encouraged to review other OLIRs listed in the catalog to better understand what is required to develop and submit an OLIR to NIST. Developers are also encouraged to contact NIST with any questions about the development and submission process at olir@nist.gov.

Patent Disclosure Notice

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

Following the ITL call for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, notice of one or more such claims has been received.

By publication, no position is taken by ITL with respect to the validity or scope of any patent claim or of any rights in connection therewith. The known patent holder(s) has (have), however, provided to NIST a letter of assurance stating either (1) a general disclaimer to the effect that it does (they do) not hold and does (do) not currently intend holding any essential patent claim(s), or (2) that it (they) will negotiate royalty-free or royalty-bearing licenses with other parties on a demonstrably nondiscriminatory basis with reasonable terms and conditions.

Details may be obtained from olir@nist.gov**.**

No representation is made or implied that this is the only license that may be required to avoid patent infringement in the use of this publication.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

1.1 Purpose and Scope

The purpose of this document is to assist Informative Reference Developers (Developers) in understanding the processes and requirements for participating in the National Online Informative References (OLIR) Program.

This document replaces National Institute of Standards and Technology (NIST) Interagency or Internal Report (IR) 8204, *Cybersecurity Framework Online Informative References (OLIR) Submissions: Specification for Completing the OLIR Template*.

Before reading this document, Developers should first read NISTIR 8278, *National Online Informative References (OLIR) Program: Program Overview and OLIR Uses* [2]. NISTIR 8278 describes the OLIR Program and explains the ever-expanding feature set, uses, and benefits of the OLIR Catalog.

1.2 Document Structure

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

- Section 2 describes the general process for developing Informative References and submitting them to NIST for inclusion in the OLIR Catalog, as well as the processes for updating and archiving Informative References.
- Section 3 provides guidance for completing the OLIR Template when submitting an Informative Reference.
- The References section lists the references for the publication.
- Appendix A contains simplistic examples of the notional logic for determining the relationship between two document element concepts.
- Appendix B contains acronyms used throughout the document.
- Appendix C provides a glossary of terminology used throughout the document.
- Appendix D displays a notional example of values for the OLIR Template.
- Appendix E defines the Participation Agreement for the OLIR Program for Developers.

2 Informative Reference Development

This section describes the general process for developing Informative References ("References") and submitting them to NIST for inclusion in the National OLIR Program's Catalog. It includes an overview of the process that NIST will follow to screen the Informative Reference submissions and publish them in the OLIR Catalog. This section also describes the process that NIST and Developers will follow to update and archive Informative References. Developers—who may be individuals, teams, or organizations—that are considering submitting Informative References to NIST should review the Participation Agreement in Appendix E. The agreement contains the administrative requirements for participating in the National OLIR Program.

2.1 OLIR Vocabulary

For the purposes of this publication, certain terms that will be discussed in greater detail later in the document are forward declared in this section to improve readability. A *Reference Document* is the source document being compared to a Focal Document. A *Focal Document* is a source document that is used as the basis for comparing an element with an element from another document. An *Informative Reference* shows the relationship(s) between the Reference Document elements and a Focal Document element. More precisely, Informative References show relationships between any number and combination of organizational concepts (e.g., Families, Functions, Categories, Subcategories, Controls, Control Enhancements) of the Focal Document and specific sections, sentences, or phrases of Reference Documents. The discrete concepts of the Focal Document shall be called *Focal Document elements*, and the specific sections, sentences, or phrases of the Reference Document shall be called *Reference Document elements*. The term 'Reference' (or 'References') used in this document is an abbreviation for the term 'Informative Reference' (or 'Informative References').

2.2 Background

The National OLIR Program evolved from a requirement to map to, between, and from NIST documents. For example, the *Framework for Improving Critical Infrastructure Cybersecurity* ("Cybersecurity Framework," "Framework") lists several related cybersecurity documents as Informative References [4]. Informative References show relationships between Functions, Categories, and Subcategories of the Cybersecurity Framework and specific sections of standards, guidelines, and best practices. Informative References can be more detailed or more general than the Functions, Categories, and Subcategories and can illustrate ways to achieve those outcomes. Informative References suggest how to use a given cybersecurity document in coordination with the Cybersecurity Framework for the purposes of cybersecurity risk management.

Historically, Informative References only appeared in the NIST Cybersecurity Framework. However, only a small subset of Informative References was published in the Cybersecurity Framework to maintain its readability. This is a common practice for many NIST resources, and the National OLIR Program scales to accommodate a greater number of Informative References and provide a more agile support model to account for the varying update cycles of all Reference Documents. This OLIR specification also provides a more robust method for clearly defining relationships between Reference Document elements and Focal Document elements.

2.3 Informative Reference Life Cycle

The Informative Reference life cycle comprises the following steps:

1. **Initial Informative Reference Development:** The Developer becomes familiar with the procedures and requirements of the National OLIR Program, performs the initial development of the Informative Reference, and refines the Informative Reference using the OLIR Validation (OLIRVal) Tool.
2. **Informative Reference Posting:** The Developer posts the Informative Reference on a publicly available site for linking.
3. **Informative Reference Submitted to NIST:** The Developer submits a package, consisting of the Informative Reference and documentation, to NIST for screening and public review.
4. **NIST Screening:** NIST screens the submission package's information, confirms that the Informative Reference conforms to this specification, and addresses any issues with the Developer prior to public review.
5. **Public Review and Feedback:** NIST holds a 30-day public review of the draft candidate Informative Reference. The Developer then addresses comments, as necessary.
6. **Final Listing in the OLIR Catalog:** NIST updates the Informative Reference listing status in the OLIR Catalog from 'draft' to 'final' and announces the Informative Reference's availability.
7. **Informative Reference Maintenance and Archival:** Anyone can provide feedback on the Informative Reference throughout its life cycle. The Developer periodically updates the Informative Reference, as necessary. The Informative Reference is archived when it is no longer maintained or needed (e.g., if the Reference Document is withdrawn or deprecated).

Each step should be carried out to ensure that the Informative Reference is accurate, well-formed, and documented during its development and subsequent publication, update, or archival. The following sections describe considerations for each step.

2.4 Developer Steps for Creating, Posting, and Submitting Informative References

The first three steps in the development methodology listed above involve the developer creating, posting, and submitting Informative References. Sections 2.4.1 through 2.4.3 describe each of these steps in greater detail.

2.4.1 Initial Informative Reference Development

During initial Informative Reference development, a Developer becomes familiar with the requirements of the National OLIR Program and all procedures involved during the Informative Reference life cycle (as described throughout Section 2). At this point, a Developer would presumably agree to the requirements for participation in the National OLIR Program before continuing to develop the Informative Reference. Appendix E of this publication provides the latest version of the Participation Agreement that SHALL be signed by the Developer.

The quality of Informative Reference documentation can significantly impact the Informative Reference's effectiveness. To promote consistency and facilitate the review of Informative References by NIST and the public, NIST has created a spreadsheet template (OLIR Template). Section 3 of this publication provides instructions and definitions for completing the OLIR Template.

2.4.2 Informative Reference Posting

Once the Informative Reference is completed using the OLIR Template, the Developer SHALL post the Informative Reference to a public website. This posting enables NIST to link to the Informative Reference during both the comment period and the listing phase. The public website should be the same website that is listed in the *General Information* tab of the Informative Reference. The website listed in the OLIR Catalog can be updated if the Informative Reference's location changes. Section 3 also indicates that the Developer SHALL use the NIST-provided OLIRVal tool to ensure that the populated OLIR Template conforms to the specifications in this publication.

2.4.3 Informative Reference Submitted to NIST

At this point, the Developer has completed and posted the Informative Reference. The Developer now sends a submission package to NIST. It SHALL consist of the following:

- Completed Informative Reference using the OLIR Template,
- Supporting documentation, and
- Signed Participation Agreement (see Appendix E).

Submission packages are sent to the National OLIR Program email alias, olir@nist.gov.

2.5 NIST Steps for Reviewing and Finalizing Informative References for Publication

The NIST process for screening and publishing an Informative Reference, which corresponds to steps 4 through 7 in the Informative Reference life cycle, is described in the following sections.

2.5.1 NIST Screening of the Submission Package

NIST reviews the submission and determines if the Informative Reference and other submitted materials are ready for public review. NIST screens the submission package for completeness and accuracy and ensures that the content is well-formed. NIST may contact the Developer with questions about the submitted materials during the screening period.

2.5.2 Public Review and Feedback for the Candidate Informative Reference

After the submission package has been screened and the Developer has addressed any issues, NIST will post a link to the Informative Reference in the OLIR Catalog as a candidate in a 'draft' status

for a 30-day public review period. NIST will invite the public to review and comment on the candidate Informative Reference and provide feedback to the Developer.[1]

An individual reviewing an Informative Reference reviewer emails olir@nist.gov to provide comments as well as other information about the reviewer's implementation environment, procedures, and other relevant information. Depending on the review, the Developer may need to respond to comments. NIST may also consult independent expert reviewers, as appropriate. Typical reasons for using independent reviewers include the following:

- NIST may decide that it does not have the expertise to determine whether the comments have been addressed satisfactorily.
- NIST may disagree with the proposed issue resolutions and seek additional perspectives from third-party reviewers.

At the end of the public review period, NIST will give the Developer 30 days to respond to comments.

2.5.3 Final Listing in the OLIR Catalog

After any outstanding issues have been addressed, NIST will change the Informative Reference status to 'final' in the OLIR Catalog and announce its availability. The listing will provide data about the Informative Reference, downloadable formats, and links to Informative Reference materials.

2.5.4 Informative Reference Maintenance and Archival

Throughout an Informative Reference's life cycle, any reviewer can submit comments or questions to olir@nist.gov. NIST will forward feedback to the Developer. Users who subscribe to the mailing list can receive announcements of updates or other issues related to an Informative Reference. The selected Informative Reference's description, in the OLIR Catalog, will contain instructions for subscribing to the mailing address list.

NIST will periodically review the catalog of Informative References to determine if individual Informative References are still relevant or if changes need to be made. If the Developer decides to update the Informative Reference at any time, NIST will announce, via a notification in the OLIR Catalog, that the Informative Reference is in the process of being updated. If the revised Informative Reference contains major changes (see Section 3.1.2 for version definitions), it will be considered as if it were a new submission and will be required to undergo the same review process as a new submission. If the Informative Reference contains minor changes, it will undergo a 30-day public comment period. If the Informative Reference contains administrative changes, no comment period is required, and the updated Informative Reference will be listed in the OLIR Catalog with an appropriate version number to annotate the update.

At the discretion of NIST or the Developer, the Informative Reference can either be archived or removed from the OLIR Catalog altogether. Typical reasons for such actions might be that the

[1] The OLIR Catalog is located at https://csrc.nist.gov/projects/olir/informative-reference-catalog.

Reference Document is no longer supported or is obsolete, or the Developer no longer wishes to provide support for the Informative Reference. Unless otherwise requested by the Developer, withdrawn Informative References will be deleted from the OLIR Catalog, and an entry will remain to indicate that an Informative Reference was previously available.

3 OLIR Template Instructions

This section provides instructions and guidance to Developers for completing the OLIR Template for an Informative Reference. [2] The Developer SHALL complete the *General Information* and *Relationships* tabs of the OLIR Template. The Developer SHALL use the OLIRVal tool to ensure syntactic compliance with the specifications in this publication and the OLIR Template.[3]

3.1 Completing the General Information Tab

Developers SHALL complete an Informative Reference description on the *General Information* tab; this metadata will be used by NIST to update the OLIR Catalog entry for the Informative Reference. Table 1 shows the fields in the *General Information* tab that Developers are to complete. Appendix D contains an example.

Table 1: General Information Tab Field Description

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.
Informative Reference Version	The version of the Informative Reference itself. The format is a string following the pattern: [major].[minor].[administrative]. The initial submission shall have an Informative Reference Version of 1.0.0.
Web Address	The URL where the Informative Reference can be found
Focal Document Version	The Focal Document version used in creating the Informative Reference. NIST recommends that Developers begin with the latest Focal Document version.[4]
Summary	The purpose of the Informative Reference
Target Audience (Community)	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")
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
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
Dependencies/Requirements	Whether the Informative Reference is used in conjunction with other Informative Reference(s) or as a stand-alone Informative Reference
Citations	A listing of source material (beyond the Reference Document) that supported development of the Informative Reference

[2] The OLIR Template spreadsheets are available at https://csrc.nist.gov/Projects/olir/focal-document-templates.
[3] The OLIRVal tool is a .jar file that can be downloaded from https://csrc.nist.gov/Projects/olir/validation-tool.
[4] This field will be modified as additional Focal Documents are added to the OLIR Program.

3.1.1 Informative Reference Name

This field refers to the name of the spreadsheet mapping elements of a Reference Document to a Focal Document. The name SHALL be human-readable. The Informative Reference Name will remain static over time.

When naming a Reference, each of the three distinct elements SHALL be included in the following order (see also Figure 1):

1. Reference Document (see Section 3.1.9)
2. Focal Document (see Section 3.1.4)
3. Reference Version (see Section 3.1.2)

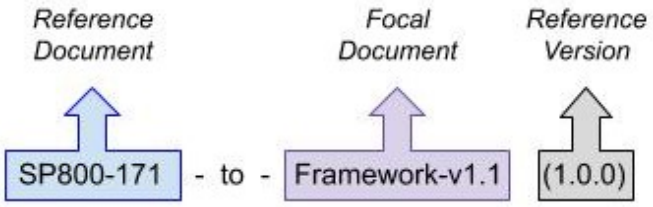

Figure 1: Informative Reference Name Elements

Spaces are replaced with hyphens except following the Focal Document; a space is used to separate the Focal Document from the Reference Version. Note that the preposition "to" separates the Reference Document from the Focal Document. Lastly, the Reference Version is contained in parentheses.

Examples:

"NIST-Privacy-Framework-v1.0-to-CSF-Framework-v1.1 (1.0.0)"

"NIST-SP800-171-to-CSF-Framework-v1.1 (1.0.0)"

"NIST-CSF-v1.1-to-NIST-SP800-53r4 (1.0.0)"

To improve user readability of Informative Reference names, Developers of References SHALL use industry-recognized abbreviations for both the Reference Document and Focal Document when naming their Reference. Developers of References MUST limit the short-form Reference Name to 35 characters. The following are examples of industry-recognized abbreviations:

- "NIST-Special-Publication-800-171" becomes "SP800-171"
- "NIST-Privacy Framework:-A-Tool-for-Improving-Privacy-Through-Enterprise-Risk-Management,-Version-1.0" becomes "Privacy-Framework-v1.0"

3.1.2 Reference Version

The Reference Version SHALL indicate a *major*, *minor*, or *administrative* designation of the Informative Reference material. Generally, the version format follows a typical software release pattern:

- *Major* version – Changes to the Informative Reference require current implementations to be modified.
- *Minor* version – Changes include one or more new mappings without the removal or modification of existing mappings.
- *Administrative* version – Changes are typographical or stylistic for usability.

The field format is **[major version].[minor version].[administrative version]**, and the initial submission SHALL use "1.0.0".

Examples: "1.0.0"; "1.1.3"; "2.0.1"

3.1.3 Web Address

The Web Address denotes the publicly available online location of the Informative Reference. It SHALL respond to standard HTTP requests.

3.1.4 Focal Document Version

The Focal Document Version is the version of the Focal Document used for the mapping. Developers SHALL use the most current version of the Focal Document when performing the mapping.

Examples: "Cybersecurity Framework v1.1; Privacy Framework v1.0; SP 800-53 Rev. 4"

3.1.5 Summary

The Summary SHOULD be a short description of the mapping exercise.

Example: "A mapping of Cybersecurity Framework version 1.1 Core to NIST Special Publication 800-53 Revision 4 controls."

3.1.6 Target Audience (Community)

The Target Audience is the intended consuming audience of the Informative Reference. The audience SHOULD be a critical infrastructure sector or community of interest. Multiple audiences are denoted by populating this field with a value of "General."

Examples: "Energy Sector"; "Legal Community"; "Restaurants"

3.1.7 Comprehensive

The Comprehensive value indicates the completeness of the Informative Reference with respect to the Focal Document. This field SHALL be marked as follows:

- "Yes" – *All* Reference Document elements in the Reference Document are mapped to the Focal Document; otherwise,
- "No" – One or more Reference Document elements in the Reference Document are *not* mapped to the Focal Document.

3.1.8 Reference Document Author

The Reference Document Author(s) refers to the organization(s) and/or person(s) who authored the Reference Document. For example, NIST would be listed as the Reference Document Author for NIST SP 800-171, even if a non-NIST Developer were to create an Informative Reference for it [5]. Multiple authors SHALL be separated by commas.

Pseudonyms and group names not registered as organization names with the Internal Revenue Service or like organizations (e.g., Doing Business As names, working group names, committee names) SHALL be listed in addition to the organizations and/or person(s) using the preface "prepared by the." Multiple pseudonyms and/or group names SHALL be separated by commas. Author(s) SHALL be separated from pseudonyms and group names using a semicolon.

Examples: "National Institute of Standards and Technology; prepared by the Joint Task Force"; "ACME, Inc."; "Jane Doe, John Smith"; "International Organization for Standardization, International Electrotechnical Commission; prepared by the Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques"

3.1.9 Reference Document

A Reference Document is any document being compared to a Focal Document. Examples include traditional documents (e.g., a formal publication in PDF format) but could also be products, services, educational materials, or training.

The Reference Document field SHALL include the full name of the Reference Document with all acronyms spelled out. The title of the publication SHALL be annotated in italics. It SHALL also include unique identifiers associated with the version, revision, and/or edition.

Examples: "Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*"; "Technical Report 27103:2018, *Information technology – Security techniques – Cybersecurity and ISO and IEC Standards"*

3.1.10 Reference Document Date

The Reference Document Date refers to the calendar date of the Reference Document version, revision, and/or edition, including any applicable amendment dates to account for any updates. The Reference Document publication and amendment dates SHALL appear in MM/DD/YYYY format. When publication and/or amendment dates list only the month and year, the day field SHALL be

recorded with "00." Publication and amendment dates SHALL be separated by a comma, and amendment dates SHALL be prepended with "updated on."

Examples: "04/00/2013, updated on 01/22/2015"; "12/00/2016"

3.1.11 Reference Document URL

This field denotes the publicly available online location of the Reference Document. It SHALL respond to standard HTTP(S) requests.

3.1.12 Informative Reference Developer

The Informative Reference Developer (Developer) is the author of the Informative Reference and may be a person, team, or organization. For example, a federal agency, product vendor, or research academic may use a Reference Document (e.g., NIST SP 800-171 [8]) and create an Informative Reference to the Cybersecurity Framework.

Example: "National Institute of Standards and Technology"; "John Doe"

3.1.13 Comments

The Developer MAY use the Comments field to provide supplemental information to NIST and other Informative Reference users. Such information may include general background information, developer's notes, or customizations made to the OLIR Template.

3.1.14 Point of Contact

The Point of Contact is a person associated with the Developer. The person named within this field SHOULD have subject matter expertise with the Informative Reference and be able to answer questions related to the Informative Reference. The format for this field is: **[First Name] [Last Name]\n+[country code] [area code]-[xxx]-[xxxx]\n[email address]**.

Example:

Jane Doe
+1 555-555-5555
example@nist.gov

3.1.15 Dependency/Requirement

If the Informative Reference being submitted is used in conjunction with other Informative Reference(s), indicate the other Informative Reference Name(s) (as they appear in their respective OLIR Catalog listings) in this field separated by a comma. Otherwise, leave the field blank.

3.1.16 Citations

The Citations field refers to documents that are supplementary to the Informative Reference. These documents may be standards or other supporting material that would prove useful to NIST or third parties. If no citations exist, leave this field blank.

Examples: "NIST Special Publication 800-53 Revision 5"; "ACME, Inc. Security Policy"

3.2 Completing the Relationships Tab

The Developer SHALL indicate the relationships between the Reference Document and the Focal Document. This information is located on the *Relationships* tab of the OLIR Template. Table 2 describes column headers for that tab.

Table 2: Relationships Tab Field Description

Field Name	Description
Focal Document Element	The identifier of the Focal Document element being mapped
Focal Document Element Description	The text description of the Focal Document element
Security Control Baseline	The identifier of the first applicable designation for a security control defined on a baseline for a low-impact, moderate-impact, or high-impact information system. This field is only applicable when utilizing the SP 800-53 Focal Document template.
Rationale	The explanation for 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 comparison 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: • 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 things that the other does not. • Equal to – 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.
Reference Document Element	The identifier of the Reference Document element being mapped
Reference Document Element Description	The description of the Reference Document element
Fulfilled By	A Boolean value indicating whether a Reference Document element fulfills the entirety of the Focal Document element
Group Identifier (optional)	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
Comments (optional)	Notes to NIST or implementers
Strength of Relationship (optional)	The extent to which a Reference Document element and a Focal Document element are similar

The *Relationships* tab of the OLIR Template contains a row for each Focal Document Element. The Developer SHALL complete the mappings for each Focal Document Element at an appropriate level to the Reference Document.

A Reference Document Element may map to any Focal Document Element. If multiple Reference Document Elements map to the same Focal Document Element, the Developer SHALL insert a row into the spreadsheet and label the Focal Document Element. Table 3 demonstrates how to correctly complete the OLIR Template in this case.

Some Focal Document Elements may not map to any Reference Document Elements. In this case, leave these rows blank. This may occur due to a different scope or level of abstraction in the Reference Document.

Some Reference Document Elements may not map to any Focal Document Elements (gaps in the Focal Document). The Developer MAY add these Reference Document Elements—a single row for each Reference Document Element—to the bottom of the OLIR Template with a relationship of "no relationship" and set the Fulfilled by field as "N." In this scenario, the Developer SHALL mark the Comprehensive field as "No" on the *General Information* tab.

3.2.1 Focal Document Element

The *Focal Document Element* refers to the element of the Focal Document that is the target of the Reference Document mapping. In the OLIR Template, the *Relationships* tab includes a row for every Focal Document element. These rows are provided for convenience only. If a Reference Document has multiple mappings to the same Focal Document element, the Developer SHALL include additional rows. Rows that are deemed unnecessary by the Developer SHALL remain blank. The format of these fields corresponds to the Focal Document element identifiers.

Examples:

"ID"; "PR"; "RC.CO"; "DE.AE-1" for the Cybersecurity Framework v1.1 Focal Document template

"ID-P"; GV-P"; "CT.PO-P"; "CM.PO-P1" for the Privacy Framework v1.0 Focal Document template

"AC-1"; "RA-1"; "SC-4 (1)" for the SP 800-53 Rev. 4 Focal Document template

Developers SHOULD map to the lowest level of abstraction in the focal document where practical, applicable, and possible. Regarding SP 800-53, the lowest level of abstraction in the Focal Document is the control enhancements rather than the control or family. For the Cybersecurity Framework, the lowest level of abstraction is the subcategories. OLIR submissions will be accepted with a combination of mapping abstractions.

3.2.2 Focal Document Element Description

The *Focal Document Element Description* field contains the text description of the Focal Document element. This description is a fixed value that is included here for convenience and readability. The Developer SHALL copy this text if additional rows are necessary.

Examples: Data at rest is protected; impact of events is determined; privacy values, policies, and training are reviewed, and any updates are communicated; the organization reviews and updates the audited events [Assignment: organization-defined frequency].

3.2.3 Security Control Baseline

This field is only applicable for a Developer utilizing the SP 800-53 Focal Document template. The Security Control Baseline field contains the identifier of the first applicable designation for a security control defined on a baseline for a low-impact, moderate-impact, or high-impact information system. The identifiers are fixed values that are included here for convenience, readability, and additional sorting capabilities for the Developer. The Developer SHALL copy this text if additional rows are necessary. The identifiers are: *Low, Moderate, High, Not Selected, Withdrawn, and Not Associated.*

3.2.4 Rationale

The explanation for why a given Reference Document element and Focal Document element are related is attributed to one of three basic reasons. In Section 3.2.5 and Appendix E, these are referred to as the "logical comparison approaches." The Developer SHALL populate the corresponding Rationale field with one of these three explanations: syntactic, semantic, or functional.

- *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 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:

  "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."

- *Functional* – Analyzes (i.e., transposes) the functions of the Reference Document element and 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]

When choosing a rationale, in general, the Developer SHOULD select the strictest applicable selection according to its provability. A syntactic rationale is the strictest; it implies a word-for-word analysis of the relationship and no interpretation of the language (this is often the case where a

document quotes from a source document). A semantic rationale implies some interpretation of the language. A functional rationale implies that the outcomes of the language have been analyzed rather than the words in the relationship. Therefore, the order of most strict to least strict rationale assertions is syntactic, semantic, then functional. The order also implies less reliance on the intention of the author and interpreter in syntactic and the most in functional assertions. See Section 3.2.5 for additional information on the interrelatedness of rationales and relationships.

3.2.5 Relationship

The *Relationship* field refers to the logical comparison between a Reference Document element and a Focal Document element. Relationships can be described using one of five cases derived from a branch of mathematics known as set theory. The relationship between the Reference Document and Focal Document elements can be *subset of*, *intersects with*, *equal*, *superset of*, or *not related to*. Figure 2 depicts these conceptual relationships.

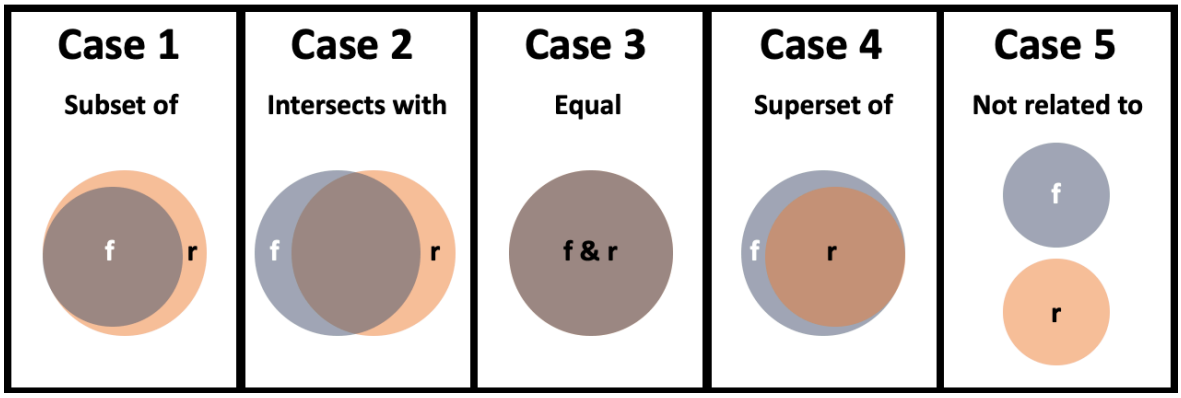

Figure 2: Informative Reference Relationship Types
(f = Focal Document element concept(s); r = Reference Document element concept(s))

A relationship SHALL be determined using one or more rationales defined in Section 3.2.4. The result of these comparative approaches is a set of concepts for the Focal Document element and the Reference Document element. These two sets of concepts are compared to determine the value of the *Relationship* field.

Appendix A contains Reference Document examples for each of the five aforementioned cases.

Relationship assertions have a natural order: equal, subset and superset, intersects with, and not related. *Equal* assertions indicate the most in common and *not related* assertions indicate nothing in common. The pairing of rationale and relationship provides the basis for a strength of relationship score, as discussed in Section 3.2.11. When selecting both rationale and relationship assertions, the developer SHOULD seek to maximize the strength of relationship score.

3.2.6 Reference Document Element

The *Reference Document Element* refers to the statement being mapped from the Reference Document. This field represents the core text or sections of text from the Reference Document. This field SHALL be populated with values that are relative to the structure of the Reference Document and that capture the content being mapped. The Developer SHOULD populate this field with

identifiers to signify sections of text relative to the Reference Document, or the Developer MAY choose to create identifiers for the Informative Reference. In other words,

> [Reference Document Element], where {Reference Document Element 1, Reference Document Element 2, Reference Document Element 3… Reference Document Element *n*} comprise the relevant Reference Document elements.

Where Reference Document identifiers include a colon (":"), the Developer SHALL create identifiers in the Informative Reference that do not use a colon.

In the instance of creating identifiers, Developers SHALL clearly identify which sections of text are being related to the Focal Document element, as described in Section 3.2.7. In other words, the Reference Document Element Description becomes a mandatory field.

Examples:

> Pertaining to ISO 27001 [6]:
>
> > [A.6.3] – Designates A.6.3 as the Reference Document element being mapped
>
> Pertaining to NIST SP 800-53 [5]:
>
> > [AC-13] – Designates AC-13 as the Reference Document element being mapped

The Informative Reference SHALL focus on the main intuitive topic of the Reference Document and Focal Document elements being compared. If a Reference Document element contains more than one main topic, the Developer SHALL decompose it into multiple, discrete Reference Document elements. In this instance, the Developer SHALL use additional sequential identifiers to clearly identify which sections of text are being related to the Focal Document element, as described in Section 3.2.9. The Reference Document Element Description also becomes a mandatory field. The Developer SHALL use the following format when creating identifiers:

> [Reference Document Element:Sequential Identifier], where {Reference Document Element 1, Reference Document Element 2, Reference Document Element 3… Reference Document Element *n*} comprise the elements of the Reference Document, and {1, 2, 3… n} describes the set of Group Sequential Identifiers.

Examples:

> Pertaining to ISO 27001 [6]:
>
> > [A.6.3:1] – Designates the 1st portion of A.6.3 being mapped
> >
> > [A.6.3:2] – Designates the 2nd portion of A.6.3 being mapped
>
> Pertaining to NIST SP 800-53 [5]:
>
> > [AC-13:3] – Designates the 3rd portion of AC-13 being mapped

Note that only one colon may be used in the identifier, specifically to separate the Reference Document element from the sequential identifier.

3.2.7 Reference Document Element Description

The *Reference Document Element Description* field SHALL be populated with the text description of a given Reference Document element. This text is used when comparing the Reference Document element to the Focal Document element.

This field is required except when the descriptive text in the Reference Document element is protected by copyright or license restrictions.

3.2.8 Fulfilled By

The *Fulfilled By* field refers to the completeness of a Reference Document element in relation to a Focal Document element. Focal Document elements that are subsets of or equal to Reference Document elements SHALL be marked "Yes." Focal Document elements which are supersets of, intersect with, or are not related to Reference Document elements SHALL be marked "No."

When populated in conjunction with groups (see Section 3.2.9), the appropriate Yes/No value is selected relative to the entire group instead of the individual Reference Document element. In these cases, the *Fulfilled By* value for each Reference Document element SHALL be the same as the collective Group value.

3.2.9 Group Identifier (Optional)

The *Group Identifier* is a value defined by the Developer. This value indicates that individual Reference Document elements are part of a group when mapped to a Focal Document element. The Developer SHOULD create a Group Identifier to indicate that a group of Reference Document elements fulfill a Focal Document element. Group Identifiers SHALL use the following Group Identifier format:

> [Focal Document Element: Group Sequential Identifier], where {ID, PR, DE, RS, RC} comprise the elements of Cybersecurity Framework Focal Document Element, and {G1, G2, G3… G*n*} describes the set of Group Sequential Elements, where ℕ represents all of the natural numbers.

The Cybersecurity Framework Focal Document element is a member of the Cybersecurity Framework Core and can correspond to any Function, Category, or Subcategory. The Group Sequential Identifier is the literal "G" followed by the sequential number, which designates the position of the group.

Examples:

> ID.BE-1:G1 – Designates the 1st Group in the ID.BE-1 Group Identifier
>
> ID.BE-3:G1 – Designates the 1st Group in the decomposed Cybersecurity Framework element ID.BE-3 Group Identifier

ID.BE-3:G2 – Designates the 2nd Group in the decomposed Cybersecurity Framework element ID.BE-3 Group Identifier

RC.MI-1:G1 – Designates the 1st (and only Group) in the RC.MI-1 Group Identifier

Note that only one colon may be used in the identifier, specifically to separate the Reference Document Element from the Group Sequential Identifier. See Table 3 in Section 3.2.12 for an example of a Group Identifier.

3.2.10 Comments (Optional)

The *Comments* field refers to any explanatory or background text that may help Informative Reference consumers understand the developer's logic. The Developer may wish to provide additional information to Informative Reference users to explain decisions made or implementation considerations. Although this field is optional, NIST strongly encourages Developers to populate this field with supporting information that informed the Reference Developer's assertions.

Examples: "Assets under consideration for this relationship are business systems"; "Developers used the DHS Critical Infrastructure definition."

3.2.11 Strength of Relationship (Optional)

The *Strength of Relationship* field refers to the extent to which a Reference Document element and a Focal Document element are similar. The Strength of Relationship field builds upon the Relationship field. As Figure 3 depicts, in a relationship such as Subset of, two elements can have a relatively strong relationship (see Case 1) or a relatively weak relationship (see Case 2). See Section 3.2.5 for additional information on how the Relationship and Rationale fields relate to the Strength of Relationship field.

The Strength of Relationship field is optional, but Developers are encouraged to use it because it can help Reference users better understand the Developer's intent. Note that the field is intended for lateral comparisons, such as the Cybersecurity Framework and the Privacy Framework, rather than comparisons of documents at vastly different levels of abstraction, such as the Cybersecurity Framework and a research paper on a topic in quantum cryptography. To designate that two documents are not lateral, a Developer SHOULD set the Strength of Relationship field to "N/A."

When specified for lateral documents, the Strength of Relationship field SHALL be an integer from 0 to 10, where 10 is the strongest and 0 is the weakest. There is no prescribed methodology for estimating a strength of relationship score. In general, a Developer using the Strength of Relationship field SHOULD use their expert judgment to assign a value based on the following criteria:

- If the two elements have an "equal" relationship, assign a score of 10.
- If the two elements have a "subset of," "superset of," or "intersects with" relationship, and
    - They are much more similar than they are dissimilar, assign a score of 7, 8, or 9.
    - They are roughly as similar as they are dissimilar, assign a score of 4, 5, or 6.
    - They are much more dissimilar than they are similar, assign a score of 1, 2, or 3.

- If the two elements have a "not related to" relationship, assign a score of 0.

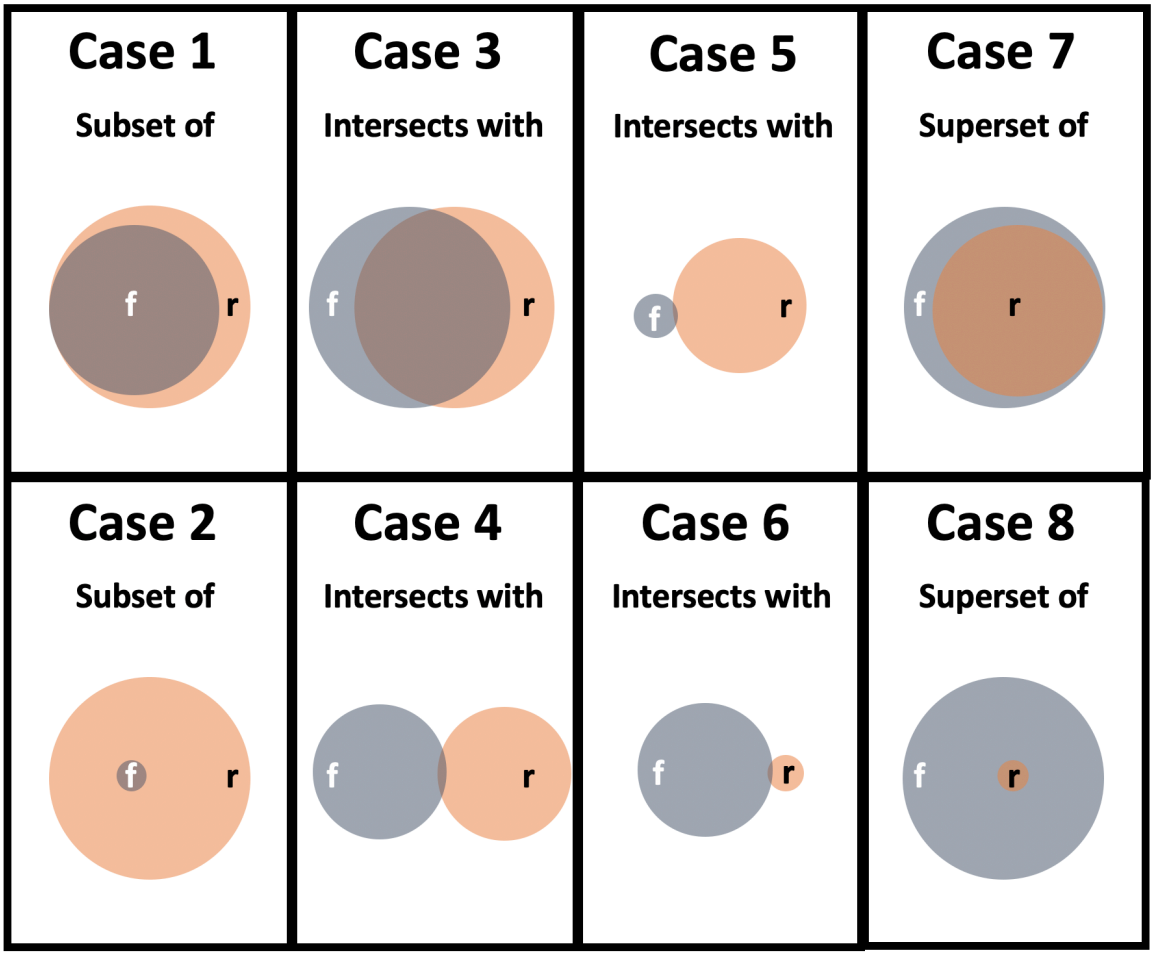

Figure 3: Relative Strength of Relationships

3.2.12 Examples of Common Scenarios

The examples in this section represent common scenarios for the Developer. They illustrate well-formed relationship rows corresponding to a fictional Reference Document.

Example 1 – Multiple Reference Document elements relate to one Cybersecurity Framework Subcategory: To designate that multiple Reference Document elements **do not** entirely fulfill the Subcategory, multiple rows SHALL *be* added as shown in Table 3. The grouping of Reference Document elements indicates a high degree of coupling. The GroupID is provided by the Developer, and in this example, the GroupID is "RS.CO-4:G1." Since the total concepts in the sets of the Refence Document elements are not greater than or equal to the total concepts in RS.CO-4, the *Fulfilled By* column is marked "No" for all rows. The high degree of coupling creates a high level of comparison for the group's strength score pertaining to RS.CO-4.

Table 3: Template Examples for Multiple Reference Document Elements

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Group ID (optional)	Strength of Relationship
RS.CO-4	Coordination with stakeholders occurs consistent with response plans.	Syntactic	superset of	1.2.3	text	N	RS.CO-4:G1	9
RS.CO-4	Coordination with stakeholders occurs consistent with response plans.	Semantic	intersects with	4.5.6	text	N	RS.CO-4:G1	9
RS.CO-4	Coordination with stakeholders occurs consistent with response plans.	Functional	superset of	7.8.9	text	N	RS.CO-4:G1	9

Example 2 – Single Reference Document element fulfills a Privacy Framework Focal Document element: This example illustrates how to document the use case when a single Reference Document element fulfills a Privacy Framework Focal Document element. Although this specific example uses a Privacy Framework Category, any Privacy Framework element can be used. Table 4 also depicts a *one-to-one* mapping in which a single Privacy Framework element is equal to a Reference Document element. This Relationship designation indicates that the Reference Document element entirely fulfills the Category.

Table 4: OLIR Template Example for a Single Reference Document Element

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Group ID (optional)	Strength of Relationship
ID.IM-P	Data processing by systems, products, or services is understood and informs the management of privacy risk.	Semantic	equal	10.11.12	text	Y		10

Example 3 – Single Reference Document element does not fulfill an SP 800-53 Focal Document element: This example illustrates how to document the use case when a single Reference Document element does not fulfill an SP 800-53 Focal Document element. Although Table 5 depicts this specific example of a single SP 800-53 Security Control element, any SP 800-53 Security/Privacy Control or control enhancement can be used. This Relationship designation indicates that the single Reference Document element does not fulfill the Focal Document element, and the strength of the relationship is weak.

Table 5: Second OLIR Template Example for a Single Reference Document Element

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Group ID (optional)	Strength of Relationship
IA-2	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Functional	Intersects with	13.14.15	text	N		2

References

[1] Bradner S (1997) Key words for use in RFCs to Indicate Requirement Levels (Internet Engineering Task Force), Request for Comments (RFC) 2119, Best Current Practice (BCP) 14. https://doi.org/10.17487/RFC2119

[2] Keller N, Quinn SD, Scarfone KA, Smith MC, Johnson V (2020) National Online Informative References (OLIR) Program: Program Overview and OLIR Uses (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8278. https://doi.org/10.6028/NIST.IR.8278

[3] National Institute of Standards and Technology (2020) *Cybersecurity Framework*. Available at https://www.nist.gov/cyberframework

[4] 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

[5] 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

[6] ISO/IEC JTC 1/SC27 (2013) ISO/IEC 27001:2013(E) – *Information technology – Security techniques – Information security management systems* (International Organization for Standardization/International Electrotechnical Commission, Switzerland), 23 pp. Available at https://www.iso.org/standard/54534.html

[7] 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

[8] 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—Relationship Examples

The notional logic for determining the relationships depicted in Figure 2 is presented in this appendix. An element concept can be an entire document, chapter or section of a document, bullet, meaning of a paragraph, description of an educational or course offering, description of a product, or service feature. While the Cybersecurity Framework is the Focal Document used to demonstrate the notional logic, any focal document could serve to demonstrate the relationship examples.

The examples below are extended explanations of the Relationships described in Section 3.2.5. The examples were taken from NIST SP 800-171, and all Reference Document elements are referenced as described in that publication [8]. All Cybersecurity Framework element examples are taken from version 1.1 of the Cybersecurity Framework [4].

Case 1 – Subset of

In Figure 2, the Venn Diagram in Case 1 refers to the scenario in which the Reference Document element contains unique concepts and shares concepts with the Cybersecurity Framework element.

Example

Cybersecurity Framework element: PR.AT-4, "Senior executives understand their roles and responsibilities."

Reference Document element: [8] requirement 3.2.2, "Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities."

This example assumes that the Developer is using a *functional* mapping technique as described in Section 3.2.4. PR.AT-4 states that a specific group of users (senior executives) should be trained on their roles and responsibilities. Requirement 3.2.2 in [8] states that "all users" should be trained on their roles and responsibilities. The Developer may assert that the concept "all users" contains the concept "senior executives and others."

Given that

a) the Reference Document element and Cybersecurity Framework element share concepts,
b) the Reference Document element contains unique concepts, and
c) the Cybersecurity Framework element does not contain unique concepts,

their designated relationship is "subset of." In other words,

"[4] element PR.AT-4 is a subset of [8] requirement 3.2.2."

Case 2 – Intersects with

In Figure 2, the Venn Diagram for Case 2 refers to the scenario in which the Cybersecurity Framework element contains unique concepts, the Reference Document element contains unique

concepts, and the Reference Document element and Cybersecurity Framework element share concepts.

Example

Cybersecurity Framework element: RS.CO-2, "Incidents are reported consistent with established criteria."

Reference Document element: [8] requirement 3.6.2, "Track, document, and report incidents to appropriate organizational officials and/or authorities."

If the Developer uses a *semantic* mapping technique as described in Section 3.2.4, the action denoted by the same concept of *documenting and reporting incidents* is accomplished. However, RS.CO-2 contains the concept of "established criteria," and [8] requirement 3.6.2 contains the concept of "appropriate organizational officials and authorities."

Given that the compared Reference Document element and Cybersecurity Framework element

a) share concepts and
b) both contain unique concepts,

their designated relationship is "intersects with." In other words,

"[4] element RS.CO-2 intersects with [8] requirement 3.6.2."

Case 3 – Equal

In Figure 2, the Venn Diagram for Case 3 refers to the scenario in which the Cybersecurity Framework element and the Reference Document element only share concepts, and neither the Reference Document nor the Cybersecurity Framework element has any unique concepts.

Example

Cybersecurity Framework element: PR.PT-3, "The principle of least functionality is incorporated by configuring systems to provide only essential capabilities."

Reference Document element: [8] requirement 3.4.6, "Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities."

If the Developer uses either a *functional* or *semantic* mapping technique as described in Section 3.2.4, the shared concept of "employing/incorporating the principle of least functionality by configuring systems to provide only essential capabilities" is considered equal. Neither the Reference Document element nor the Cybersecurity Framework element contains any unique concepts.

Given that the Reference Document element and Cybersecurity Framework element

a) share all concepts and
b) contain no unique concepts,

their designated relationship is "equal." In other words,

"[4] element PR.PT-3 is equal to [8] requirement 3.4.6."

Case 4 – Superset of

In Figure 2, the Venn Diagram for Case 4 refers to the scenario in which the Cybersecurity Framework element contains unique concepts and shares concepts with the Reference Document element.

Example

Cybersecurity Framework element: PR.AC-1, "Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes."

Reference Document element: [8] requirement 3.5.1, "Identify system users, processes acting on behalf of users, and devices."

If the Developer uses a *functional* mapping technique to issue a credential as described in Section 3.2.4, a process or user would have to be identified. While [8] requirement 3.5.1 contains this identification, the management, verification, revocation, and audit of the credential are also contained in the Cybersecurity Framework element.

Given that

a) the Reference Document element and Cybersecurity Framework element share concepts,
b) the Cybersecurity Framework element contains unique concepts, and
c) the Reference Document element does not contain unique concepts,

their designated relationship is "superset of." In other words,

"[4] element PR.AC-1 is a superset of [8] requirement 3.5.1."

Case 5 – Not related to

In Figure 2, the Venn Diagram for Case 5 refers to the scenario in which the Cybersecurity Framework element and the Reference Document element do not share any concepts. Some Reference Document elements may not relate to any Cybersecurity Framework elements, so the former may be omitted or marked "Not related to," along with a blank Cybersecurity Framework Element field. If a Reference Document element is omitted entirely from the OLIR Template, it will be assumed to be "not related to" any Cybersecurity Framework element.

Appendix B—Acronyms

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

BCP	Best Current Practice
FOIA	Freedom of Information Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IR	Interagency or Internal Report
ITL	Information Technology Laboratory
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
OLIR	Online Informative References
OLIRVal	Online Informative References Validation (Tool)
RFC	Request for Comment
SP	Special Publication
URL	Uniform Resource Locator

Appendix C—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.
OLIR Catalog	The OLIR Program's online site for sharing OLIRs.
OLIR Template	A spreadsheet that contains the fields necessary for creating a well-formed Informative Reference for submission to the OLIR Program. It serves as the starting point for the Developer.
Online Informative Reference (OLIR)	An Informative Reference expressed in NISTIR 8278A-compliant format and shared by the OLIR Catalog.
Rationale	The explanation for why a Reference Document element and a Focal Document element are related. This will be one of the following: Syntactic, Semantic, or Functional.
Reference	See *Informative Reference*.
Reference Document	A source 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.
Reference Version	The version of the Informative Reference.

Relationship	The type of logical comparison that the Reference Document Developer asserts compared to the Focal Document. This will be one of the following: subset of, intersects with, equal to, superset of, or not related to.
Strength of Relationship	The extent to which a Reference Document element and a Focal Document element are similar.
User	A person, team, or organization that accesses or otherwise uses an Online Informative Reference.

Appendix D—General Information Example

The table below displays field values that adhere to the specification within Section 3.1.

Field Name	Field Value
Informative Reference Name	NIST-SP800-171-to-Framework-v1.1 (1.0.0)
Reference Version	1.0.0
Web Address	http://www.nist.gov/files/xxxxxx
Focal Document Version	Cybersecurity Framework v1.1
Summary	The purpose of this Informative Reference is to provide a relationship between NIST SP 800-171 and the Cybersecurity Framework.
Target Audience (Community)	The intended audience for this Informative Reference is those seeking to protect controlled unclassified information using the Cybersecurity Framework.
Comprehensive	Yes
Reference Document Author	National Institute of Standards and Technology
Reference Document	Special Publication 800-171, Revision 1: *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
Reference Document Date	12/00/2016, updated on 06/07/2018
Reference Document URL	https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
Reference Developer	National Institute of Standards and Technology
Comments	None
Point of Contact	Jane Doe +1 555-555-5555 example@nist.gov
Dependency/Requirement	This Informative Reference is a stand-alone Reference and does not have any dependencies.
Citations	Mapping of Cybersecurity Framework v.1.0 to SP 800 171 Rev. 1, https://csrc.nist.gov/CSRC/media//Publications/sp/800-171/rev-1/final/documents/csf-v1-0-to-sp800-171rev1-mapping.xlsx

Appendix E—Participation Agreement for the NIST OLIR Program

In order to submit a candidate Informative Reference to NIST, an Informative Reference submitter must first review, sign, and submit a Participation Agreement. That form establishes the terms of agreement for participating in the NIST National Online Informative References (OLIR) Program.

Participation Agreement
The NIST National Online Informative References Program

Version 1.2
June 11, 2020

The phrase "NIST National Online Informative References Program" is intended for use in association with specific documents for which a candidate Informative Reference (Reference) has been created and that meet the requirements of the Program for final listing upon submission to the Informative Reference catalog. You may participate in the Program if you agree in writing to the following terms and conditions:

1. Informative References are made reasonably available.
2. You will follow the expectations of the Program as detailed in NIST Interagency Report 8278A, Section 2.
3. You will respond to comments and issues raised by a public review of your Informative Reference submission within 30 days of the end of the public review period. Any comments from reviewers and your responses may be made publicly available.
4. You agree to maintain the Informative Reference and provide a timely response (within 10 business days) to requests from NIST for information or assistance regarding the contents or structure of the Informative Reference.
5. You represent that, to the best of your knowledge, the use of your Informative Reference submission will not infringe on any intellectual property or proprietary rights of third parties. You will hold NIST harmless in any subsequent litigation involving the Informative Reference submission.
6. You may terminate your participation in the Program at any time. You will provide 10 business days' notice to NIST of your intention to terminate participation. NIST may terminate its consideration of an Informative Reference submission or your participation in

the Program at any time. NIST will contact you 10 business days prior to its intention to terminate your participation. You may, within five business days, appeal the termination and provide convincing supporting evidence to rebut that termination.

7. You may not use the name or logo of NIST or the Department of Commerce on any advertisement, product, or service that is directly or indirectly related to this participation agreement.
8. NIST does not directly or indirectly endorse any product or service provided or to be provided by you, your successors, assignees, or licensees. You may not in any way imply that participation in this Program is an endorsement of any such product or service.
9. Your permission for advertising participation in the Program is conditioned on and limited to those Informative References and the specific Informative Reference versions for which an Informative Reference is made currently available by NIST through the Program on its Final Informative References List.
10. Your permission for advertising participation in the Program is conditioned on and limited to those Informative Reference submitters who provide assistance and help to users of the Informative Reference with regard to the proper use of the Informative Reference and that the warranty for the Informative Reference and the specific Informative Reference versions is not changed by use of the Informative Reference.
11. NIST reserves the right to charge a participation fee in the future. No fee is required at present. No fees will be made retroactive.
12. NIST may terminate the Program at its discretion. NIST may terminate your participation in the Program for any violation of the terms and conditions of the program or for statutory, policy, or regulatory reasons. This Participation Agreement does not create legally enforceable rights or obligations on behalf of NIST.

By signing below, the developer agrees to the terms and conditions contained herein.

_____

Organization or company name

_____

Name and title of organization authorized person

_____

Signature

_____

Date