Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date November 20, 2020

Original Release Date August 4, 2020

Superseding Document

Status Final

Series/Number NIST Interagency or Internal Report 8278A

Title National Cybersecurity Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers

Publication Date November 2020

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

CSRC URL https://csrc.nist.gov/publications/detail/nistir/8278a/final

Additional Information OLIR homepage: https://csrc.nist.gov/projects/olir

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

1 **Draft NISTIR 8278A**

2
National Cybersecurity Online Informative References (OLIR)
3
Program:
4

5 *Submission Guidance for OLIR Developers*

6 Matthew Barrett
7 Nicole Keller
8 Stephen Quinn
9 Matthew Smith
10 Karen Scarfone

11
12
13
16

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

National Cybersecurity Online Informative References (OLIR) Program

18

19

20

Submission Guidance for OLIR Developers

21

22   Matthew Barrett*   Matthew Smith
23   *Applied Cybersecurity Division*   *Huntington Ingalls Industries*
24   *Information Technology Laboratory*   *Annapolis Junction, MD*

25   Nicole Keller   Karen Scarfone
26   Stephen Quinn   *Scarfone Cybersecurity*
27   *Computer Security Division*   *Clifton, VA*
28   *Information Technology Laboratory*
29
30   *Former employee; all work for this publication was done while at NIST*

31

32

35

36 August 2020

37

65   **Reports on Computer Systems Technology**

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

74   **Abstract**

75   The National Cybersecurity Online Informative References (OLIR) Program is a NIST effort to
76   facilitate subject matter experts in defining standardized Online Informative References (OLIRs),
77   which are relationships between elements of their documents and elements of other documents
78   like the NIST Cybersecurity Framework. This document assists Informative Reference
79   Developers in understanding the processes and requirements for participating in the Program.
80   The primary focus of the document is to instruct Developers on how to complete the OLIR
81   Template spreadsheet when submitting an Informative Reference to NIST for inclusion in the
82   OLIR Catalog. This document replaces IR 8204, *Cybersecurity Framework Online Informative*
83   *References (OLIR) Submissions: Specification for Completing the OLIR Template.*

84   **Keywords**

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

89   **Audience**

90   The primary audience for this publication is individuals interested in developing Informative
91   References for the National Cybersecurity OLIR Program.

92   **Trademark Information**

93   All registered trademarks and trademarks belong to their respective organizations.

94

95 **Document Conventions**

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

101 **Note to Reviewers**

102 Section 3.2.11 of this draft is on "strength of relationship." This section was added due to
103 feedback from early adopters as well as discussion at the OLIR workshop. The feedback
104 received was that the options for "relationship" lacked detail in describing the relative magnitude
105 of the two elements. Based on suggestions from early adopters and discussions with subject
106 matter experts, the current "strength of relationship" section attempts to bring additional clarity
107 to element relationships.

108 NIST is interested in perspectives relating to the proposed approach to "strength of relationship."
109 Of particular interest are answers to the following questions:

110 • Does the phrase "strength of relationship" accurately capture the concept?

111 • Does the approach provide value to users?

112 • Are there more effective approaches which capture the concept or provide value to users?
113 In particular, what methodologies might be beneficial?

114

115   **Call for Patent Claims**

116   This public review includes a call for information on essential patent claims (claims whose use
117   would be required for compliance with the guidance or requirements in this Information
118   Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be
119   directly stated in this ITL Publication or by reference to another publication. This call also
120   includes disclosure, where known, of the existence of pending U.S. or foreign patent applications
121   relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.
122
123   ITL may require from the patent holder, or a party authorized to make assurances on its behalf,
124   in written or electronic form, either:
125
126   a) assurance in the form of a general disclaimer to the effect that such party does not hold
127   and does not currently intend holding any essential patent claim(s); or
128
129   b) assurance that a license to such essential patent claim(s) will be made available to
130   applicants desiring to utilize the license for the purpose of complying with the guidance
131   or requirements in this ITL draft publication either:
132
133   i.   under reasonable terms and conditions that are demonstrably free of any unfair
134   discrimination; or
135   ii. without compensation and under reasonable terms and conditions that are
136   demonstrably free of any unfair discrimination.
137
138   Such assurance shall indicate that the patent holder (or third party authorized to make assurances
139   on its behalf) will include in any documents transferring ownership of patents subject to the
140   assurance, provisions sufficient to ensure that the commitments in the assurance are binding on
141   the transferee, and that the transferee will similarly include appropriate provisions in the event of
142   future transfers with the goal of binding each successor-in-interest.
143
144   The assurance shall also indicate that it is intended to be binding on successors-in-interest
145   regardless of whether such provisions are included in the relevant transfer documents.
146
147   Such statements should be addressed to: olir@nist.gov
148

149 **Table of Contents**

212   **List of Tables**

218

219

220 **1   Introduction**

221 **1.1   Purpose and Scope**

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

225 This document replaces IR 8204, *Cybersecurity Framework Online Informative References*
226 *(OLIR) Submissions: Specification for Completing the OLIR Template.*

227 Before reading this document, Developers should first read National Institute of Standards and
228 Technology (NIST) Interagency or Internal Report (IR) 8278, *National Cybersecurity Online*
229 *Informative References (OLIR) Program: Program Overview and OLIR Uses* ("NISTIR 8278")
230 [2]. NISTIR 8278 describes the OLIR Program and explains the uses and benefits of the OLIR
231 Catalog.

232 **1.2   Document Structure**

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

234   • Section 2 describes the general process for developing Informative References and
235   submitting them to NIST for inclusion in the OLIR Catalog, as well as the processes for
236   updating and archiving Informative References.

237   • Section 3 provides guidance for completing the OLIR Template when submitting an
238   Informative Reference.

239   • The References section lists the references for the publication.

240   • Appendix A contains simplistic examples of the notional logic for determining the
241   relationship between two document element concepts.

242   • Appendix B contains acronyms used throughout the document.

243   • Appendix C provides a glossary of terminology used throughout the document.

244   • Appendix D displays a notional example of values for the OLIR Template.

245   • Appendix E defines the Participation Agreement for the OLIR Program for Developers.

246

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 Cybersecurity OLIR Program's OLIR 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 Informative Reference Developers ("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 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 exactly, Informative References show relationships between any number and combination of organizational concepts (e.g., 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 *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 are often more detailed than the Functions, Categories, and Subcategories and 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 have only appeared in the Cybersecurity Framework document; only a smaller subset of Informative References is published in that document to maintain its readability. The National Cybersecurity OLIR Program scales to accommodate a greater number of Informative References and provides 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.

285   **2.3   Informative Reference Life Cycle**

286   The Informative Reference life cycle comprises the following steps:

287   1. **Initial Informative Reference Development**: The Developer becomes familiar with the
288   procedures and requirements of the OLIR Program, performs the initial development of the
289   Informative Reference, and refines the Informative Reference using the OLIR Validation
290   (OLIRVal) Tool.

291   2. **Informative Reference Posting**: The Developer posts the Informative Reference on a
292   publicly available site for linking.

293   3. **Informative Reference Submitted to NIST**: The Developer submits a package, consisting
294   of the Informative Reference and documentation, to NIST for screening and public review.

295   4. **NIST Screening**: NIST screens the submission package's information, confirms that the
296   Informative Reference conforms to this specification, and addresses any issues with the
297   Developer prior to public review.

298   5. **Public Review and Feedback**: NIST holds a 30-day public review of the draft candidate
299   Informative Reference. The Developer then addresses comments, as necessary.

300   6. **Final Listing in the OLIR Catalog**: NIST updates the Informative Reference listing status
301   in the OLIR Catalog from 'draft' to 'final' and announces the Informative Reference's
302   availability.

303   7. **Informative Reference Maintenance and Archival**: Anyone can provide feedback on the
304   Informative Reference throughout its life cycle. The Developer periodically updates the
305   Informative Reference, as necessary. The Informative Reference is archived when it is no
306   longer maintained or needed (e.g., if the Reference Document is withdrawn or deprecated).

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

310   **2.4   Developer Steps for Creating, Posting, and Submitting Informative References**

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

314   **2.4.1   Initial Informative Reference Development**

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

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

326   **2.4.2   Informative Reference Posting**

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

334   **2.4.3   Informative Reference Submitted to NIST**

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

337   •   Completed Informative Reference using the OLIR Template,

338   •   Supporting documentation, and

339   •   Signed Participation Agreement (see Appendix E).

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

341   **2.5   NIST Steps for Reviewing and Finalizing Informative References for Publication**

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

344   **2.5.1   NIST Screening of the Submission Package**

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

349   **2.5.2   Public Review and Feedback for the Candidate Informative Reference**

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

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

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

359 • NIST may decide that it does not have the expertise to determine whether the comments have
360   been addressed satisfactorily.

361 • NIST may disagree with the proposed issue resolutions and seek additional perspectives from
362   third-party reviewers.

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

2.5.3 Final Listing in the OLIR Catalog

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

2.5.4 Informative Reference Maintenance and Archival

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

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

386 At the discretion of NIST or the Developer, the Informative Reference can either be archived or
387 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/Cybersecurity-Framework/Informative-Reference-Catalog.

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

392 **3   OLIR Template Instructions**

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

397 **3.1   Completing the General Information Tab**

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

402   **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://www.nist.gov/cyberframework/informative-references/validation-tool.
[3] The OLIRVal tool is a .jar file that can be downloaded from https://www.nist.gov/cyberframework/informative-references/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.

For naming a Reference, each of the three distinct elements MUST 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)
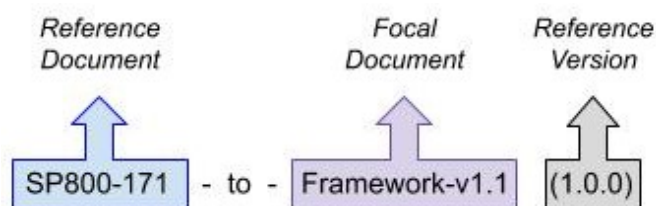
Figure 1: Informative Reference Name Elements

Spaces are replaced with hyphens except following the Focal Document; a space is used to separate the Focal Document from the Reference Version. Please 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-Framework-v1.1 (1.0.0)"

"NIST-SP800-171-to-Framework-v1.1 (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:

432   • *Major* version – Changes to the Informative Reference require current implementations to be
433   modified.

434   • *Minor* version – Changes include one or more new mappings, without the removal or
435   modification of existing mappings.

436   • *Administrative* version – Changes are typographical or stylistic for usability.

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

439   *Examples:* "1.0.0"; "1.1.3"; "2.0.1".

3.1.3   Web Address

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

3.1.4   Focal Document Version

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

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

3.1.5   Summary

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

450   *Example:* "A mapping of Cybersecurity Framework version 1.1 Core to NIST Special Publication
451   800-53 Revision 4 controls."

3.1.6   Target Audience (Community)

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

456   *Examples:* "Energy Sector"; "Legal Community"; "Restaurants".

3.1.7   Comprehensive

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

460   • "Yes" – *All* Reference Document elements in the Reference Document are mapped to the
461   Focal Document; otherwise,

9

462   • "No" – One or more Reference Document elements in the Reference Document are *not*
463   mapped to the Focal Document.

3.1.8   Reference Document Author

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

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

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

3.1.9   Reference Document

479   A Reference Document is any document being compared to a Focal Document. Examples include
480   traditional documents, products, services, educational materials, and training.

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

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

3.1.10   Reference Document Date

488   The Reference Document Date refers to the calendar date of the Reference Document version,
489   revision, and/or edition, including any applicable amendment dates to account for any updates. The
490   Reference Document publication and amendment dates SHALL appear in MM/DD/YYYY format.
491   When publication and/or amendment dates list only the month and year, the day field SHALL be
492   recorded with a "00." Publication and amendment dates SHALL be separated by a comma, and
493   amendment dates SHALL be prepended with "updated on."

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

495   **3.1.11 Reference Document URL**

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

498   **3.1.12 Reference Developer**

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

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

504   **3.1.13 Comments**

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

508   **3.1.14 Point of Contact**

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

513   *Example:*

514   Jane Doe
515   +1 555-555-5555
516   example@nist.gov
517
518   **3.1.15 Dependency/Requirement**

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

522   **3.1.16 Citations**

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

526   *Examples:* "NIST Special Publication 800-53 Revision 4"; "ACME, Inc. Security Policy".

527 **3.2 Completing the Relationships Tab**

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

531 **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

532 The *Relationships* tab of the OLIR Focal Document template contains a row for each Focal
533 Document element. The Developer SHALL complete the mappings for each Focal Document
534 element at an appropriate level to the Reference Document.

535 A Reference Document element may map to any Focal Document element. If multiple Reference
536 Document elements map to the same Focal Document element, the Developer SHALL insert a row

537   into the spreadsheet and label the Focal Document element. Table 3 demonstrates how to correctly
538   complete the OLIR Template in this case.

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

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

3.2.1   Focal Document Element

548   The *Focal Document Element* refers to the Focal Document element that is the target of the
549   Reference Document mapping. In the OLIR Template, the *Relationships* tab includes a row for every
550   Focal Document element. These rows are provided for convenience only. If a Reference Document
551   has multiple mappings to the same Focal Document element, the Developer SHALL include
552   additional rows. Rows that are deemed unnecessary by the Developer SHALL remain blank. The
553   format of these fields corresponds to the Focal Document element identifiers. For example, the first
554   three columns of Table 2 of the Cybersecurity Framework source document include unique
555   identifiers used as the format within the Cybersecurity Framework Focal Document element field.

556   *Examples*:

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

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

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

3.2.2   Focal Document Element Description

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

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

3.2.3   Security Control Baseline

569   This field is only applicable for a Developer utilizing the SP 800-53 Focal Document template. The
570   Security Control Baseline field contains the identifier of the first applicable designation for a
571   security control defined on a baseline for a low-impact, moderate-impact, or high-impact

572   information system. The identifiers are fixed values that are included here for convenience,
573   readability, and additional sorting capabilities for the Developer. The Developer SHALL copy this
574   text if additional rows are necessary. The identifiers are: *Low, Moderate, High, Not Selected,*
575   *Withdrawn, and Not Associated.*

576   3.2.4   Rationale

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

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

585   printf ("bar");   [… C programming language]

586   printf ("bar");   [… C programming language]

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

591   "Organization employs a firewall at the network perimeter"

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

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

598   printf ("foo\n");   [… C programming language]

599   print "foo"   [… BASIC programming language]

600   When choosing a rationale, in general, the Developer SHOULD select the strictest applicable
601   selection according to its provability. A syntactic rationale is the strictest; it implies a word-for-word
602   analysis of the relationship and no interpretation of the language (this is often the case where a
603   document quotes from a source document). A semantic rationale implies some interpretation of the
604   language. A functional rationale implies that the outcomes of the language have been analyzed rather
605   than the words in the relationship. Therefore, the order of most strict to least strict rationale
606   assertions is syntactic, semantic, then functional. The order also implies less reliance on the intention

607 of the author and interpreter in syntactic and the most in functional assertions. See Section 3.2.5 for
608 additional information on the interrelatedness of rationales and relationships.

3.2.5 Relationship

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

615
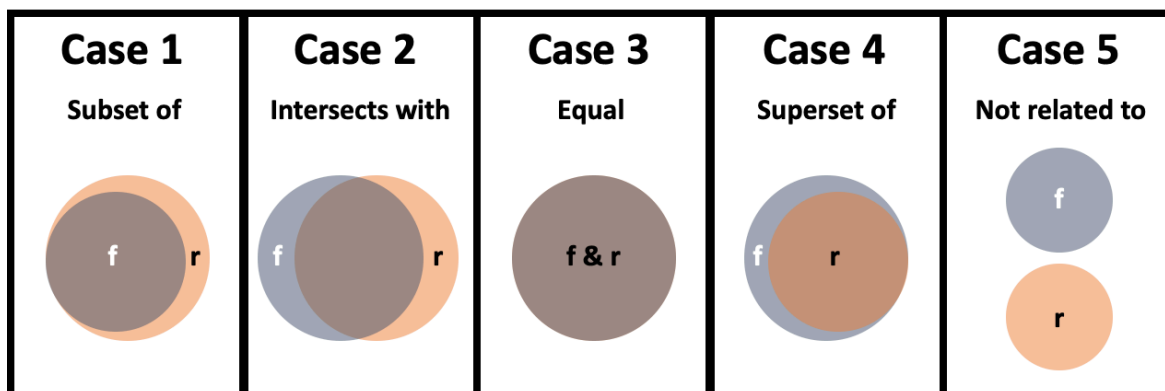
616 **Figure 2: Informative Reference Relationship Types**
617 *(f = Focal Document element concept(s); r = Reference Document element concept(s))*

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

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

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

3.2.6 Reference Document Element

629 The *Reference Document Element* refers to the statement being mapped from the Reference
630 Document. This field represents the core text or sections of text from the Reference Document. This
631 field SHALL be populated with values relative to the structure of the Reference Document that
632 capture the content being mapped. The Developer SHOULD populate this field with identifiers to
633 signify sections of text relative to the Reference Document, or the Developer MAY choose to create
634 identifiers for the Informative Reference. In other words,

635   [Reference Document Element] where { Reference Document Element 1, Reference
636   Document Element 2, Reference Document Element 3… Reference Document Element n},
637   comprise the relevant Reference Document elements.

638   Where Reference Document identifiers include a colon, the Developer SHALL create identifiers in
639   the Informative Reference that do not use the colon.

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

643   Examples:

644   Pertaining to ISO 27001 [6]:

645   [A.6.3] - Designates A.6.3 as the Reference Document element being mapped

646   Pertaining to NIST SP 800-53 [5]:

647   [AC-13] - Designates AC-13 as the Reference Document element being mapped

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

655   [Reference Document Element:Sequential Identifier] where {Reference Document Element
656   1, Reference Document Element 2, Reference Document Element 3… Reference Document
657   Element n}, comprise the elements of the Reference Document, and {1, 2, 3… n} describes
658   the set of Group Sequential Identifiers.

659   Examples:

660   Pertaining to ISO 27001 [6]:

661   [A.6.3:1] - Designates the 1st portion of A.6.3 being mapped

662   [A.6.3:2] - Designates the 2nd portion of A.6.3 being mapped

663   Pertaining to NIST SP 800-53 [5]:

664   [AC-13:3] - Designates the 3rd portion of AC-13 being mapped

665   Note that only one colon (":") may be used in the identifier, specifically to separate the Reference
666   Document element from the sequential identifier.

667   **3.2.7   Reference Document Element Description**

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

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

673   **3.2.8   Fulfilled By**

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

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

682   **3.2.9   Group Identifier (Optional)**

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

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

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

696   ID.BE-1:G1 – Designates the 1st Group in the ID.BE-1 Group Identifier

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

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

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

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

3.2.10 Comments (Optional)

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

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

3.2.11 Strength of Relationship (Optional)

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

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

726   When specified for lateral documents, the Strength of Relationship field SHALL be an integer from
727   0 to 10, where 10 is the strongest and 0 is the weakest. There is no prescribed methodology for
728   estimating a strength of relationship score. In general, a Developer using the Strength of
729   Relationship field SHOULD use their expert judgment to assign a value based on the following
730   criteria:

731   • If the two elements have an "equal" relationship, assign a score of 10.

732   • If the two elements have a "subset of," "superset of," or "intersects with" relationship, and

733   o they are much more similar than they are dissimilar, assign a score of 7, 8, or 9.

734   o they are roughly as similar as they are dissimilar, assign a score of 4, 5, or 6.

735   o they are much more dissimilar than they are similar, assign a score of 1, 2, or 3.

736   • If the two elements have a "not related to" relationship, assign a score of 0.
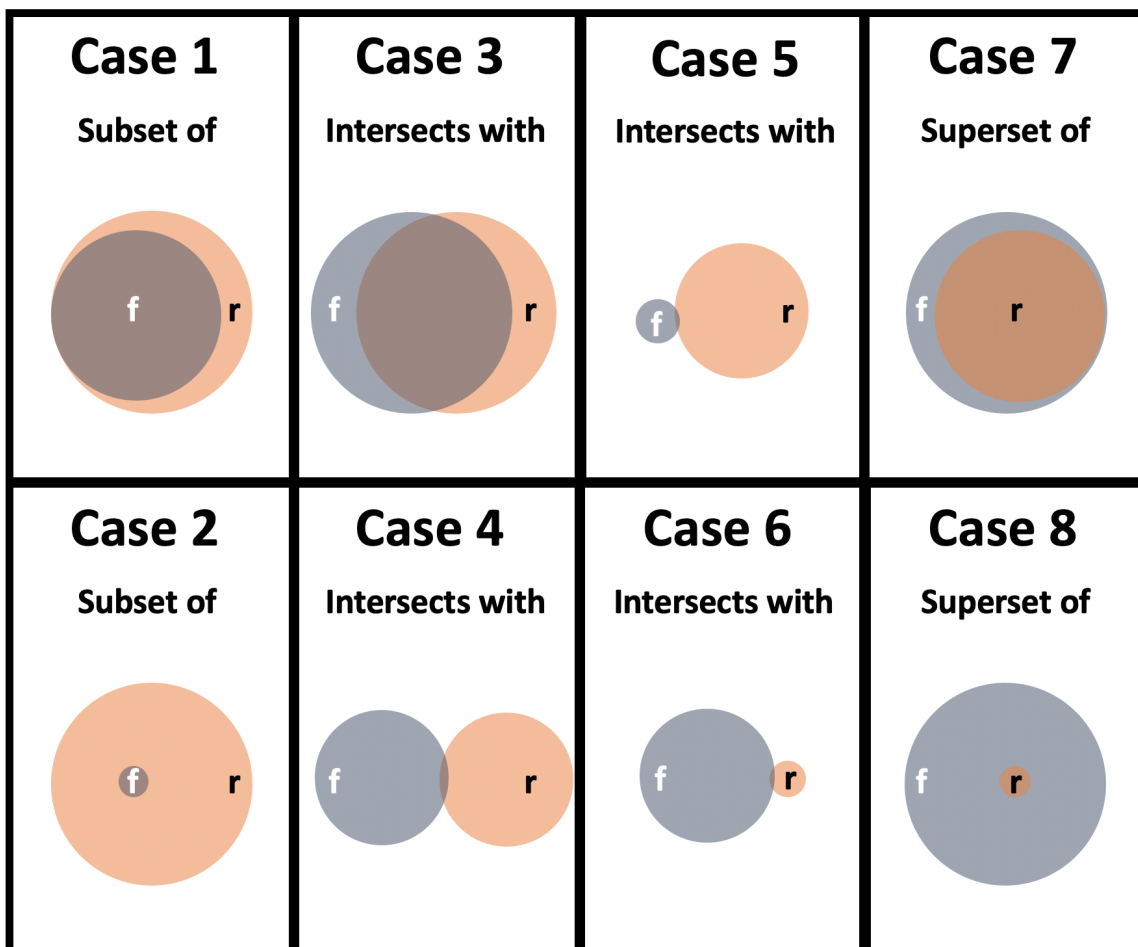
Figure 3: Relative Strength of Relationships

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.

750   **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

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

758   **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

759

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

767   **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

768
769

770   **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 S, Scarfone K, Smith M, Johnson V (2020) National Cybersecurity 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-draft2

[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. 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

771
772

773   **Appendix A—Relationship Examples**

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

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

783   **Case 1 – Subset of**

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

786   ***Example***

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

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

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

797   Given that

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

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

803   "[4] element PR.AT-4 is a subset of [8] requirement 3.2.2."

804   **Case 2 – Intersects with**

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

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

809 ***Example***

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

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

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

818 Given that the compared Reference Document element and Cybersecurity Framework element

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

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

822   "[4] element RS.CO-2 intersects with [8] requirement 3.6.2."

823 **Case 3 – Equal**

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

827 ***Example***

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

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

832 If the Developer uses either a *functional* or *semantic* mapping technique as described in Section
833 3.2.4, the shared concept of "employing/incorporating the principle of least functionality by
834 configuring systems to provide only essential capabilities" is considered equal. Neither the
835 Reference Document element nor the Cybersecurity Framework element contains any unique
836 concepts.

837 Given that the Reference Document element and Cybersecurity Framework element

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

24

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

841   "[4] element PR.PT-3 is equal to [8] requirement 3.4.6."

842   **Case 4 – Superset of**

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

846   *Example*

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

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

851   If the Developer uses a *functional* mapping technique to issue a credential as described in Section
852   3.2.4, a process or user would have to be identified. While [8] requirement 3.5.1 contains this
853   identification, the management, verification, revocation, and audit of the credential are also
854   contained in the Cybersecurity Framework element.

855   Given that

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

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

861   "[4] element PR.AC-1 is a superset of [8] requirement 3.5.1."

862   **Case 5 – Not related to**

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

869

870   **Appendix B—Acronyms**

871   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

872

873 **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 of 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 specific section, sentence, or phrase 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.

874

875   **Appendix D—General Information Example**

876   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 the NIST SP 800-171 document 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 standalone 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

877

878   **Appendix E—Participation Agreement for the NIST OLIR Program**

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

883
884   **Participation Agreement**
885   **The NIST National Cybersecurity Online Informative References Program**

886   **Version 1.2**
887   **June 11, 2020**

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

893   1. Informative References are made reasonably available.

894   2. You will follow the expectations of the Program as detailed in NIST Interagency Report
895   8278A, Section 2.

896   3. You will respond to comments and issues raised by a public review of your Informative
897   Reference submission within 30 days of the end of the public review period. Any comments
898   from reviewers and your responses may be made publicly available.

899   4. You agree to maintain the Informative Reference and provide a timely response (within 10
900   business days) to requests from NIST for information or assistance regarding the contents or
901   structure of the Informative Reference.

902   5. You represent that, to the best of your knowledge, the use of your Informative Reference
903   submission will not infringe on any intellectual property or proprietary rights of third parties.
904   You will hold NIST harmless in any subsequent litigation involving the Informative
905   Reference submission.

906   6. You may terminate your participation in the Program at any time. You will provide two
907   business weeks' notice to NIST of your intention to terminate participation. NIST may

908   terminate its consideration of an Informative Reference submission or your participation in
909   the Program at any time. NIST will contact you two business weeks prior to its intention to
910   terminate your participation. You may, within one business week, appeal the termination and
911   provide convincing supporting evidence to rebut that termination.

912   7. You may not use the name or logo of NIST or the Department of Commerce on any
913   advertisement, product, or service that is directly or indirectly related to this participation
914   agreement.

915   8. NIST does not directly or indirectly endorse any product or service provided or to be
916   provided by you, your successors, assignees, or licensees. You may not in any way imply
917   that participation in this Program is an endorsement of any such product or service.

918   9. Your permission for advertising participation in the Program is conditioned on and limited to
919   those Informative References and the specific Informative Reference versions for which an
920   Informative Reference is made currently available by NIST through the Program on its Final
921   Informative References List.

922   10. Your permission for advertising participation in the Program is conditioned on and limited to
923   those Informative Reference submitters who provide assistance and help to users of the
924   Informative Reference with regard to the proper use of the Informative Reference and that
925   the warranty for the Informative Reference and the specific Informative Reference versions
926   is not changed by use of the Informative Reference.

927   11. NIST reserves the right to charge a participation fee in the future. No fee is required at
928   present. No fees will be made retroactive.

929   12. NIST may terminate the Program at its discretion. NIST may terminate your participation in
930   the Program for any violation of the terms and conditions of the program or for statutory,
931   policy, or regulatory reasons. This Participation Agreement does not create legally
932   enforceable rights or obligations on behalf of NIST.

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

934   _____
935   Organization or company name

936   _____
937   Name and title of organization authorized person

938   _____
939   Signature

940   _____
941   Date
942