DRAFT NISTIR 8204

Cybersecurity Framework Online Informative References (OLIR) Submissions

Specification for Completing the OLIR Template

Matthew Barrett
Stephen Quinn
Matthew Smith

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

DRAFT NISTIR 8204

Cybersecurity Framework Online Informative References (OLIR) Submissions

Specification for Completing the OLIR Template

Matthew Barrett
Applied Cybersecurity Division
Information Technology Laboratory

Stephen Quinn
Computer Security Division
Information Technology Laboratory

Matthew Smith
G2, Inc.
Annapolis Junction, Maryland

May 2018

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 Internal Report 8204
30 pages (May 2018)

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

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

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

Public comment period: *May 17, 2018* through *July 16, 2018*

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

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

Reports on Computer Systems Technology

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

Abstract

This document provides instructions and definitions for completing the Cybersecurity Framework (CSF) Online Informative References (OLIR) spreadsheet template available for download at https://www.nist.gov/cyberframework/informative-references. This document is intended to assist developers of References as a companion document to the spreadsheet template. Definitions are provided for column and row headings in addition to a discussion of expected values.

Keywords

Crosswalk; Cybersecurity Framework; Informative References; Framework for Improving Critical Infrastructure Cybersecurity; Mapping; Online Informative References; References; Template Population;

Acknowledgments

The authors would like to thank Nicole Keller, Lisa Carnahan, Murugiah Souppaya, Vince Johnson, Jeff Marron, and Jim Foti for sharing their excellent thoughts and guiding the concepts and prose of this report.

Audience

Developers of Informative References to the Cybersecurity Framework.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Reference Development

This section describes the general process for developing References and submitting them to the Reference catalog. It includes a cursory overview of the process NIST will follow to screen the Reference submissions and publish them in its repository, and the process NIST and developers will follow to update or archive the References. Individual developers and organizations that want to submit References to NIST should review the Participation Agreement (Appendix E), which contains the administrative requirements for participation in the References Program. Before submitting a Reference to NIST, developers should ensure they have the most recent version of this document[1].

1.1 Background

The *Framework for Improving Critical Infrastructure Cybersecurity*[2] (Cybersecurity Framework, Framework) lists several related cybersecurity documents as Informative References (References). References show relationships between the Cybersecurity Framework Functions, Categories, and Subcategories and specific sections of standards, guidelines, and best practices. References are often more detailed than the Functions, Categories, and Subcategories and illustrate ways to achieve those outcomes. References suggest how to use a given cybersecurity document in coordination with the Framework for the purposes of cybersecurity risk management.

Historically, References have only appeared in the Cybersecurity Framework document. To maintain readability of the document, a smaller subset of References is published in the Cybersecurity Framework. Online Informative References (OLIR) scales to accommodate a greater number of 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 of defining relationships with the Cybersecurity Framework.

1.2 Reference Lifecycle

The Reference life cycle comprises the following steps:

1. **Initial Reference Development**: The developer becomes familiar with the procedures and requirements of the Reference Program, and then performs the initial development of the Reference.
2. **Reference Posting**: The developer posts the Reference on a publicly available site for linking.
3. **Reference Submitted to NIST**: The developer submits the Reference and documentation package to NIST for screening and public review.

[1] The latest updated participation agreement is located at https://www.nist.gov/sites/default/files/documents/2018/02/14/online_informative_reference_program_participation_agreement_form_20171005.pdf. This updated material should be consulted before formally agreeing to participate in the program.

[2] The Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

4. **NIST Screening**: NIST screens the Reference package's information and confirms the submission is well-formed, then addresses any issues with the developer prior to public review.
5. **Public Review and Feedback**: NIST holds a 30-day public review of the candidate Reference. Then the developer addresses comments as necessary.
6. **Final Listing on Reference Repository**: NIST lists the Reference, by way of website update, in the repository as final and announces the Reference's availability.
7. **Reference Maintenance and Archival**: Anyone can provide feedback on the Reference throughout its life cycle. The developer updates the Reference periodically as necessary. The Reference is archived when it is no longer maintained or is no longer needed.

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

1.3 Developer Steps for Creating, Posting, and Submitting References

The first three steps in the development methodology listed above involve the developer creating, posting, and submitting References. Sections 1.1.1 through 1.1.3 describe each of these steps in greater detail.

1.3.1 Initial Reference Development

During initial Reference development, a developer becomes familiar with the requirements of the Reference program and all procedures involved during the Reference life cycle (as described throughout this section). At this point, a developer and developer organization would presumably agree to the requirements for participation in the References Program before continuing to develop the Reference.

The quality of Reference documentation can significantly impact the Reference's effectiveness. Section 2.0 of this document provides instructions and definitions for completing the Reference template.

1.3.2 Reference Posting

Once the Reference is created, the developing organization should post the Reference to a public website. This posting enables NIST to link to the Reference during both the comment period and the listing phase. This website should be the same website as is listed in the *General Information* tab of the Reference. The website can change from posting to listing.

1.3.3 Reference Submittal to NIST

At this point, the Reference developer has completed and posted the Reference. The developer now submits the package of materials to NIST. The package includes the following:

- Completed Reference Template Spreadsheet,
- Supporting documentation, and

- Signed participation agreement (see Appendix E).

Reference packages are submitted to NIST through the Cybersecurity Framework OLIR References email alias at cyberframework-refs@nist.gov.

1.4 NIST Steps for Reviewing and Finalizing References for Publication

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

1.4.1 NIST Screening of the Reference Package

This step involves determining if the submitted Reference materials are ready for public review. NIST screens the Reference package for completeness, accuracy, and ensures that content is well-formed (see Section 2). NIST may contact the developer with questions about the submitted materials during the screening period.

1.4.2 Public Review and Feedback for the Candidate Reference

After the Reference package has been screened and the developer has addressed any issues, NIST will post the Reference as a candidate draft and announce a 30-day public review period. NIST will invite the public to review and comment on the Reference submission and provide feedback to the Reference developers. Feedback may be incorporated in a revision of the Reference to improve its quality. When a candidate Reference has completed the review process, its information is added to the Reference repository.

A Reference reviewer emails cyberframework-refs@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 Reference 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 reviews from third parties to get additional perspectives.

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

1.4.3 Final Listing on Reference Repository

After any outstanding issues have been addressed, NIST lists the final Reference and announces that the Reference is now listed on the repository. The listing will provide high level data as well as a link to the Reference, hosted by the developer.

1.4.4 Reference Maintenance and Archival

Throughout a Reference's life cycle, any reviewer can provide comments or ask questions regarding the Reference by mailing cyberframework-refs@nist.gov. NIST will pass feedback to the Reference developer. NIST may maintain a mailing address for the associated References. Users who subscribe to the mailing list can receive announcements of updates or other issues connected with a Reference. The selected Reference's description (on the Reference repository) will contain instructions for subscribing to the mailing address list.

After the final Reference is listed, NIST will periodically review the Reference to determine if it is still relevant or if changes need to be made to it. If the developer decides to update the Reference at any time, NIST will announce that the Reference is in the process of being updated. If the revised Reference contains major changes, it will be accepted as if it were a new submission and will be required to undergo the same review process as a new submission.

At NIST's or the developer's discretion, the Reference can be removed from the repository or marked as an archive. Typical reasons for such actions would be that the Reference source document is no longer supported or is obsolete, or that the developer no longer wishes to provide support for the Reference.

1.4.5 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 [RFC2119]. When these words appear in regular case, such as "should" or "may", they are not intended to be interpreted as RFC 2119 key words.

2 Reference Template Instructions

This section provides guidance to Reference developers for completing the Reference template. The Reference developer SHALL complete both tabs of the Reference template spreadsheet workbook including the *General Information* and *Relationships*. A well-formed Reference submission will have all fields in the *General Information* tab complete and one or more rows of relationships in the *Relationships* tab. The following sections provide instructions and guidance for populating the Reference template.

2.1 Completing the General Information Tab

Reference developers SHALL complete an online Reference description which is the first tab in the spreadsheet workbook template labeled *General Information*.[3] 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 Reference will be referred. The format is a human readable string of characters
Reference Version	The version of the Reference itself. The format is a string following the pattern: [major].[minor].[administrative]. The initial submission shall have a Reference Version of 1.0.0.
Web Address	URL where the mapping can be found
Cybersecurity Framework Version	Framework version used in creating the mapping. It is recommended that Reference developers begin with Framework version 1.1. The format is a string following the pattern: [major].[minor].[administrative]
Mapping Summary	The purpose of the Reference
Target Audience (Community)	The intended audience for the Reference
Comprehensive (Y/N)	Whether the Reference addresses all Cybersecurity Framework elements within the Reference document. Either “Yes” or “No”
Reference Author	The organization(s) which created the Reference
Reference Document Author	The organization(s) which created the Reference document
Comments	Notes to NIST or to implementers
Point of Contact	At least one person's name, email address, and phone number within the Reference Author organization
Dependency/ Requirement	Whether the Reference is used with other Reference(s), or as a stand-alone Reference
Citations	A listing of source material (beyond the Reference document) which supported development of the Reference

The developer SHALL complete the fields describing the Reference accurately.

[3] An offline version of the Spreadsheet Template description form can be downloaded from the Reference Participation Materials site at https://www.nist.gov/file/421906.

2.1.1 Informative Reference Name

Informative Reference Name refers to the name of the source reference material. The name SHALL be human readable. The Informative Reference name remains static over time.

Examples: “HIPAA Security Rule Mapping”; “SP 800-53 Revision 4”.

2.1.2 Reference Version

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

- *Major* version: changes to the 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].

The initial submission of the Reference SHALL use “1.0.0”.

Examples: “1.0.0”; “1.1.3”; “2.0.1”.

2.1.3 Web Address

Web Address denotes the publicly available, online location of the Reference; it SHALL respond to standard HTTP(S) GET requests.

Examples: https://www.nist.gov/file/372651; https://cyber.securityframework.org/files/file/23-uoc-framework-use-case/.

2.1.4 Cybersecurity Framework Version

The Cybersecurity Framework Version is the version of the Cybersecurity Framework used for the mapping. Developers SHALL use the most current version of the Cybersecurity Framework at https://www.nist.gov/cyberframework when performing the mapping.

It is RECOMMENDED that developers begin with Framework version 1.1.

Examples: “1.0”; “1.1”.

2.1.5 Mapping Summary

The Mapping Summary should be a short description of the mapping exercise.

For example: “A mapping of Cybersecurity Framework version 1.1 Core to NIST Special Publication 800-53 revision 4 controls”.

2.1.6 Target Audience (Community)

The Target Audience is the intended consuming audience of the Reference mapping. 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”.

2.1.7 Comprehensive

The Comprehensive value indicates the completeness of the Reference, with respect to the Cybersecurity Framework document. This field SHALL be marked as follows:

- “Yes”: *all* elements in the Reference document are mapped to the Cybersecurity Framework document; otherwise,
- “No”: at least one element in the Reference document is *not* mapped to the Cybersecurity Framework document.

2.1.8 Reference Author

The Reference Author is the person or organization that developed the Reference. For example, a federal agency, product vendor or research academic may use a Reference Document (i.e. SP800-53) and create references to the Cybersecurity Framework.

Example: “National Institute of Standards and Technology”; “John Doe”.

2.1.9 Reference Document Author

The Reference Document Author(s) refers to the author of the Reference document. For example, NIST authored the SP800-53 and it may be used by a Reference Author to create References to the Cybersecurity Framework.

Examples: “National Institute of Standards and Technology”; “ACME, Inc.”.

2.1.10 Comments

The Comments field can include information that (e.g., background knowledge, developers notes, or customizations made to the Reference template) which the Reference developer would like to provide NIST outside of the currently required information.

2.1.11 Point of Contact

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

Example:

Jane Doe
+1 555-555-5555
janedoe@acme.com.

2.1.12 Dependency/Requirement

The Dependency/Requirement refers to the ecosystem in which the Reference resides. If the Reference being submitted is used in conjunction with another Reference, input the Reference Name(s) of the Reference into the field, comma separated. Otherwise, leave the field blank.

2.1.13 Citations

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

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

2.2 Completing the Relationships Tab

Reference developers SHALL complete the Reference relationships to the Reference document. This information is located on the second tab of the Reference template spreadsheet labeled *Relationships*. Table 2 (below) describes column headers for this tab of the spreadsheet workbook.

Table 2: Relationships Tab Field Description

Field Name	Description
Framework Element	The identifier of the Cybersecurity Framework Core element being mapped
Framework Element Description	The text explaining the Cybersecurity Framework Core element.
Rationale	The processes, principles, or methods used to map the Reference document element to the Cybersecurity Framework Core element
Relationship	The type of logical relationship the Reference document element asserts compared to the Cybersecurity Framework Core element target. This value may be one of 5 options {superset, subset, equivalent, intersects, no relationship}
Reference Document Element	The identifier of the Reference document element being mapped
Reference Document Element Description (optional)	The description of the Reference document element
Fulfilled By (Y/N)	Boolean value indicating whether a Reference document element fulfills the entirety of the Cybersecurity Framework Core element
Group Identifier (optional)	The designation given to a Reference document element when the element is part of a group of reference elements that correlates to a Cybersecurity Framework Core element
Comments (optional)	Additional information useful to NIST or the implementer of the Reference

The *Relationships* tab of the Reference template spreadsheet contains a row for each Function, Category, and Subcategory of the Cybersecurity Framework Core. Reference developers SHALL complete the mappings for each Framework element at an appropriate level to the Reference document.

A Reference document element may map to a Function, Category, or Subcategory. If multiple Reference document elements map to the same Framework element, the developer SHALL insert a row into the spreadsheet and label the Framework element. Table 3 demonstrates how to correctly complete the Reference template in this case.

Some Framework elements may not map to any Reference document elements (gaps in the Reference document). In this case, leave these rows blank. This may occur due to the different levels of abstraction and focus on Reference documents being compared.

Some Reference document elements may not map to any Framework elements (gaps in the Framework). At the Reference developer's discretion, these elements can be added, a single row for each element, to the bottom of the Reference template with a relationship of "no relationship". In this scenario, the Reference developer should ensure that the Comprehensive field on the *General Information* tab of the spreadsheet is marked "No."

2.2.1 Framework Element

The *Framework Element* refers to the Cybersecurity Framework Core element that is the target of the Reference document mapping. The Reference template provides a row in the Relationships tab of the spreadsheet for every Cybersecurity Framework element; where Function, Category, and Subcategory are represented. These rows are provided for convenience only. If a Reference has multiple mappings to the same Cybersecurity Framework Core element, additional rows SHALL be added by the developer. Rows that are deemed unnecessary by the Reference developer SHALL remain blank. The format of these fields corresponds to the Cybersecurity Framework Core element identifiers found in Table 2 of the Cybersecurity Framework source document.

Examples: "ID"; "PR"; "RC.CO"; "DE.AE-1".

2.2.2 Framework Element Description

The *Framework Element Description* refers to the text descriptions of the Cybersecurity Framework Core element. These descriptions are fixed values that are for convenience and readability. Developers shall copy this text if new rows are necessary to complete the Reference. Examples: Data at rest is protected; impact of events is determined.

2.2.3 Rationale

The explanation of why a given Reference document element and Cybersecurity Framework element are related is attributed to one of three basic reasons.

Syntactic – Analyzes the linguistic meaning of the two elements to develop the conceptual comparison sets. Syntactic analysis uses literal analysis of (translates) the elements.

> *Example 1*: A syntactic mapping might be established between the following phrases to allow a Reference developer to assert “please pass me a tissue” and “pass me a tissue, please.”

> *Example 2*: A syntactic mapping might be established between the following common phrases: “Make a copy of this paper” and “Copy this paper.”

Semantic – Analyzes the contextual meaning of the two elements to develop the conceptual comparison sets. Semantic analysis interprets (transliterates) the language within the elements

> *Example 1*: A semantic mapping might be established between the following phrases to allow a Reference developer to assert “please pass me a tissue” and “please pass me a Kleenex.”

> *Example 2*: A semantic mapping might be established between the following common phrases: “Use the copier machine” and “Use the XEROX machine.”

Functional – Analyzes (transposes) the functions of the two elements to develop the conceptual comparison sets. Functional analysis may be akin to “subject matter expertise.”

> *Example 1*: A functional mapping might be established between the following phrases to allow a Reference developer to assert “I need a tissue” and “please pass me a Kleenex.”

> *Example 2*: A functional mapping might be established between the following common phrases: “Make a copy of this paper” and “XEROX this paper.”

The corresponding *Rationale* field SHALL be populated with one of the three above explanations – *syntactic*, *semantic*, or *functional*. The rationale SHOULD be considered in identifying and describing the *Relationship*.

2.2.4 Relationship

The *Relationship* field refers to the logical comparison between Reference elements and the Cybersecurity Framework Core elements. The relationships represent a one-way mapping from the Reference document to the Framework which is read left to right. While this may seem counterintuitive for the developer, it results in a more user-friendly and consumable finished document.

Relationships can be described using one of five cases derived from a branch of mathematics known as set theory. The relationship of Reference elements to Cybersecurity Framework Core elements can be: *subset of*, *intersects with*, *equivalent to*, *superset of*, or *not related to*. Figure 1 depicts these relationships.

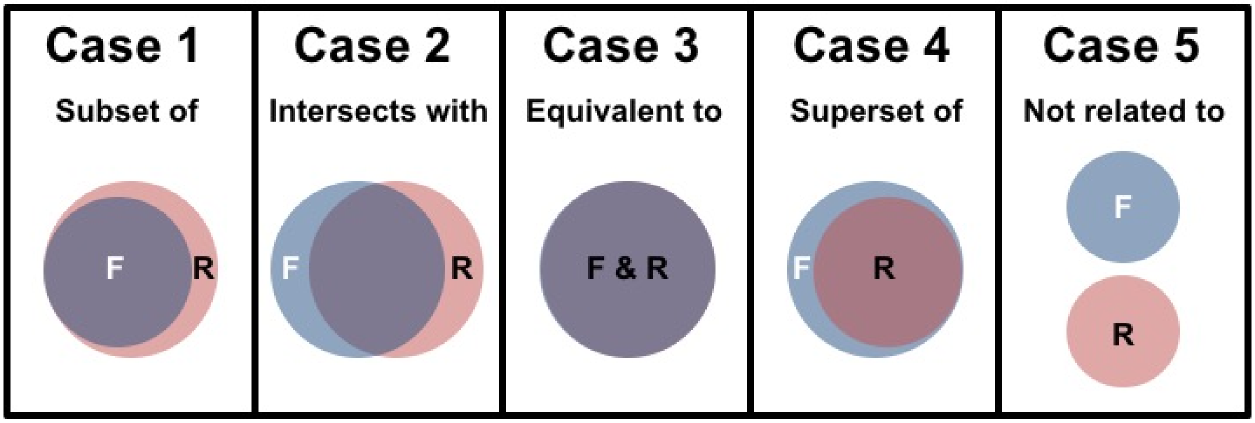

Figure 1 - Reference Relationship Types
(F = Framework elements; R = Reference elements)

Determining the relationship of a Reference element can employ multiple logical comparison approaches that are defined in Section 2.2.4.1. The result of these comparative approaches is a set of concepts for the Framework element and the Reference document element. These two sets of concepts are compared to determine the value of the relationship field. The logic for determining relationships depicted in Figure 1 is presented below:

$$where\ F\ is\ the\ set\ of\ all\ Framework\ elements\ and\ R\ is\ the\ set\ of\ all\ Reference\ document\ elements,$$

$$Framework\ element\ concepts = C_F = \{m_1(f) \mid f \in F\}$$

$$Reference\ document\ element\ concepts = C_R = \{m_2(r) \mid r \in R\}$$

$$Shared\ concepts = C_S = C_F \cap C_R$$

Note that m_1, m_2 may be the same mapping function/process/procedure. It is recommended they are the same.

Also note that all examples are derived from NIST SP 800-171 and all elements are referenced as described in that publication.

2.2.4.1 Case 1 – Subset of

In Figure 1, the Venn Diagram in for Case 1 refers to the scenario where the Reference document element contains unique concepts and shares concepts with the Framework element.

$$if\ C_S = C_F\ and\ \ C_R - C_S \neq \emptyset, then\ Relationship = "subset\ of"$$

Example

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

Reference document element: NIST SP 800-171 requirement 3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

$$C_F = m(\text{PR.AT-4}) = \left\{\begin{matrix} \text{senior executives,} \\ \text{training,} \\ \text{roles,} \\ \text{responsibilities} \end{matrix}\right\}$$

$$C_R = m(\ 3.2.2) = \left\{\begin{matrix} \text{senior exectives,} \\ \text{training,} \\ \text{roles,} \\ \text{responsibilities,} \\ \text{managers,} \\ \text{operational staff} \end{matrix}\right\}$$

$$C_S = C_F \cap C_R \ = \left\{\begin{matrix} \text{senior executives,} \\ \text{training,} \\ \text{roles,} \\ \text{responsibilities} \end{matrix}\right\}$$

$$C_S = C_F$$

$$C_R - C_S = \left\{\begin{matrix} \text{managers,} \\ \text{operational staff} \end{matrix}\right\} \neq \emptyset \rightarrow \text{"subset of"}$$

This example assumes the Reference Author is using a functional mapping technique as described in Section 2.2.4.1. PR.AT-4 suggests a specific group of users (Senior executives) should be trained on their roles and responsibilities. SP 800-171 requirement 3.2.2 suggests all users should be trained on their roles and responsibilities. Since all users contains Senior executives and others, this relationship is a “subset of.”

2.2.4.2 Case 2 – Intersects with

In Figure 1, the Venn Diagram for Case 2 refers to the scenario in which the Framework element contains unique concepts, the Reference document element contains unique concepts, and the two elements share concepts.

$$if\ C_F - C_S \neq\ \emptyset\ \ and\ \ C_R - C_S \neq \emptyset, then\ Relationship = \text{"}intersects\ with\text{"}$$

Example

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

Reference document element: NIST SP 800-171 requirement 3.6.2 Track, document, and report incidents to appropriate organizational officials and/or authorities.

$$C_F = m(RS.CO\text{-}2) = \left\{ \begin{matrix} incidents, \\ report, \\ established\ criteria \end{matrix} \right\}$$

$$C_R = m(3.6.2) = \left\{ \begin{matrix} track, \\ document, \\ incidents, \\ report, \\ appropriate\ organizational\ officals, \\ authorities \end{matrix} \right\}$$

$$C_S = \left\{ \begin{matrix} incidents, \\ report \end{matrix} \right\}$$

$$C_F - C_S = \{established\ criteria\} \neq \emptyset$$

$$C_R - C_S = \left\{ \begin{matrix} track, \\ document, \\ appropriate\ organizational\ officials, \\ authorities \end{matrix} \right\} \neq \emptyset \rightarrow \text{"}intersects\ with\text{"}$$

If the Reference Author is using a syntactic mapping as described in Section 2.2.4.1, the shared concepts are incidents and reporting. However, RS.CO-2 contains the concept of “established criteria” and NIST SP800-171 requirement 3.6.2 contains the concepts of “track,” “document,” “appropriate organizational officials,” and “authorities.” Given that the elements being compared share concepts in addition to each element possessing unique concepts, the relationship designation results in a value of “intersects with.”

2.2.4.3 Case 3 – Equivalent to

In Figure 1, the Venn Diagram for Case 3 refers to the scenario in which the Framework element and the Reference document element only share concepts.

$$if\ C_S = C_F = C_R, then\ Relationship = \text{"}equivalent\ to\text{"}$$

Example

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

Reference document element: NIST SP 800-171 requirement 3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

$$C_F = m(PR.PT\text{-}3) = \left\{ \begin{matrix} principle\ of\ least\ functionality, \\ configuring\ systems, \\ provide\ essential\ capabilities \end{matrix} \right\}$$

$$C_R = m(3.4.6) = \left\{ \begin{matrix} principle\ of\ least\ functionality, \\ configuring\ systems, \\ provide\ essential\ capabilities \end{matrix} \right\}$$

$$C_S = \left\{ \begin{matrix} principle\ of\ least\ functionality, \\ configuring\ systems, \\ provide\ essential\ capabilities \end{matrix} \right\}$$

$$C_S = C_F = C_R \rightarrow "Equivalent\ to"$$

This example shows two elements which are equivalent based on functional and semantic definitions described in Section 2.2.4.1.

2.2.4.4 Case 4 – Superset of

In Figure 1, the Venn Diagram for Case 4 refers to the scenario in which the Framework element contains unique concepts and shares concepts with the Reference document element.

$$if\ C_S = C_R \quad and\ C_F - C_S \neq \emptyset, then\ Relationship = \ "superset\ of"$$

Example

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

Reference document element: NIST SP 800-171 requirement 3.5.1 Identify system users, processes acting on behalf of users, and devices.

$$C_F = m(PR.AC\text{-}1) = \left\{ \begin{matrix} identities, \\ credentials, \\ identified, \\ issued, \\ managed, \\ verified, \\ revoked, \\ audited, \\ authorized\ users, \\ authorized\ devices, \\ authorized\ processes \end{matrix} \right\}$$

$$C_R = m(3.5.1) = \left\{ \begin{matrix} identified, \\ authorized\ users, \\ authorized\ devices \end{matrix} \right\}$$

$$C_S = \left\{ \begin{matrix} identified, \\ authorized\ users, \\ authorized\ devices \end{matrix} \right\}$$

$$C_S = C_R$$

$$C_F - C_S = \left\{ \begin{matrix} identities, \\ credentials, \\ issued, \\ managed, \\ verified, \\ revoked, \\ audited, \\ authorized\ processes \end{matrix} \right\} \neq \emptyset \rightarrow "superset\ of\ "$$

If the Reference Author was using a functional mapping technique, this example would be marked as “superset of”. To issue a credential, a process or user would have to be identified. While NIST SP 800-171 requirement 3.5.1 contains this identification, the management, verification, revocation, and audit of the credential is also contained in the Framework element.

2.2.4.5 Case 5 – Not related to

In Figure 1, the Venn Diagram for Case 5 refers to the scenario in which the Framework element and the Reference document element do not share any concepts. Some Reference document elements may not relate to any Framework elements; these Reference document elements may be omitted or marked “Not related to” with a blank Framework Element field. If the reference element is omitted, it will be assumed to be not related.

$$if\ C_S \neq \emptyset, then\ Relationship = "Not\ Related\ to"$$

2.2.5 Reference Document Element

The *Reference Document Element* refers to the element being mapped from the Reference document. This field represents the core text, or sections of text, from the Reference document. This field should be populated with values relative to the structure of the Reference document that captures the content being mapped. Reference developers may populate this field with identifiers to signify sections of text relative to their Reference document. Reference developers may choose to create identifiers for the Reference. In the latter case, Reference developers SHALL clearly identify which sections of text are being related to the Cybersecurity Framework Core element as described in Section 2.2.5. In other words, the Reference Document Element Description becomes a mandatory field.

[Reference Document Element] where {Reference Element 1, Reference Element 2, Reference Element 3… Reference Element n}, comprise the elements of the Reference Document

Examples:

Pertaining to ISO 27001:

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

Pertaining to SP 800-54 Revision 4

[AC-13] - Designates SP 800-53 Revision 4 AC-13 as the element being mapped.

Reference developers may choose to decompose Reference Document Elements into more discrete parts. In this instance, Reference developers SHALL use additional Sequential Identifiers to clearly identify which sections of text are being related to the Cybersecurity Framework Core element as described in Section 2.2.5. In this instance, the Reference Document Element Description becomes a mandatory field. Reference developers shall use the following format when creating identifiers:

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

Examples:

Pertaining to ISO 27001:

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

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

Pertaining to SP 800-54 Revision 4

[AC-13:3] - Designates the 3rd element of SP 800-53 Revision 4 AC-13 being mapped.

Note that only one colon ":" may be used in the identifier and specifically to separate the Reference Document Element from the Sequential Identifier.

2.2.6 (Optional) Reference Document Element Description

The *Reference Document Element Description* field should be populated with the text of a given Reference document element. This text is used when comparing the Reference Document to the Cybersecurity Framework Core element. For some Reference developers, this text may be protected under copyright and not included in the Reference.

This field is optional except when no native Reference Document Element identifier is available or when Sequential Identifiers are used to decompose the Reference Document Element beyond its native identifiers (see Section 2.2.4).

2.2.7 Fulfilled By

The *Fulfilled By* field refers to the completeness of a Reference document element in relation to a Cybersecurity Framework Core element. Framework elements which are subsets or equivalent to Reference document elements should be marked "Yes." Framework 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 2.2.7), the appropriate Yes/No value is selected relative to the whole group, not the individual element. In these cases, all *Fulfilled By* values for each element SHALL *be* populated with the collective Group value.

2.2.8 (Optional) Group Identifier

The *Group identifier* is a value defined by a Reference developer-defined. This value indicates that individual Reference document elements are part of a group when mapped to the Cybersecurity Framework element. The developer SHOULD create a Group Identifier to signify a group of Reference document elements fulfill a Cybersecurity Framework Core element. Group Identifiers SHALL use the following Group Identifier format:

$$Group\ Identifier = I = f{:}\mathrm{G}n \mid f \in F, n \in \mathbb{N}$$

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

The Framework element is a member of the Framework Core and can correspond with 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.AM-1:G1 – Designates the 1st in the ID.BE-1 Group Identifier

ID.BE-3:G1 – Designates the 1st Group in the ID.-BE-3 Group Identifier

ID.BE-3:G2 – Designates the 2nd Group in the ID.BE-3 Group Identifier

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

See Table 3 in Section 2.2.10 for an example of a Group Identifier.

2.2.9 (Optional) Comments

The *Comments* field refers to any explanatory or background text that may help the implementer to understand the developer’s logic. The Reference developer may wish to provide additional information to the implementer or NIST to explain decisions made or implementation considerations.

Examples: “Assets under consideration for this relationship are business systems.”, “Developers used the DHS Critical Infrastructure definition.”

2.2.10 Examples of Common Scenarios

The examples in this section represent common scenarios for the Reference developer. These examples illustrate well-formed relationship rows corresponding to a fictional Reference document.

Example 1 - Multiple Reference document elements relate to one Subcategory: To designate 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 Reference developer and in this example the GroupID is “RS.CO-4:G1”. Since the total of the 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 column is marked “No” for all rows.

Table 3: Template Examples for Multiple References

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

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

Table 4: Template Example for Single References

Framework Element	Framework Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description (optional)	Fulfilled By (Y/N)	Group ID (optional)
PR.DS	Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	Semantic	equivalent to	10.11.12	text	Y	

Appendix A—Acronyms

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

DE	Detect
DE.AE	Detect, Anomalies and Events
DHS	Department of Homeland Security
HIPAA	Health Insurance Portability and Accountability Act
ID	Identify
ISO	International Organization for Standardization
OLIR	Online Informative References
PR	Protect
PR.AC	Protect, Access Control
PR.AT	Protect, Awareness and Training
PR.DS	Protect, Data Security
PR.PT	Protect, Protective Technology
NIST	National Institute of Standards and Technology
RC	Recover
RC.CO	Recover, Communications
RS	Respond
RS.CO	Respond, Communications
SP	Special Publication
URL	Universal Resource Locator

Appendix B—Glossary

Informative reference

A well-formed, completed Reference template that was submitted to and accepted by NIST. These References map a Reference document to the Cybersecurity Framework.

Reference developer

A person, team, or organization that creates a Reference.

Reference document

The document compared to the Framework.

Reference template

The starting point for a Reference developer. This file contains the necessary fields to create a well-formed Reference for submission to the OLIR.

Appendix C—Bibliography

Cybersecurity Framework, National Institute of Standards and Technology [Web site], https://www.nist.gov/cyberframework [accessed 5/10/18]

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018. https://doi.org/10.6028/NIST.CSWP.04162018 [accessed 5/10/18]

NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013 (including updates as of January 15, 2014), 460pp. https://doi.org/10.6028/NIST.SP.800-53r4 [accessed 5/10/18]

NIST Special Publication (SP) 800-171 Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2016, 83pp. https://doi.org/10.6028/NIST.SP.800-171r1 [accessed 5/10/18]

International Organization for Standardization/International Electrotechnical Commission, *Information technology – Security techniques – Information security management systems*, ISO/IEC 27001:2013, September 2013. https://www.iso.org/standard/54534.html [accessed 5/10/18]

Appendix D—General Information Example

Field Name	Field Value
Informative Reference Name	NIST SP 800-171 Reference
Reference Version	1.0.0
Web Address	nist.gov/files/xxxxxx
Cybersecurity Framework Version	1.1
Mapping Summary	The purpose of this Reference is to provide a relationship between the NIST SP 800-171 document and the Framework.
Target Audience (Community)	The intended audience for this Reference is security managers and those seeking to implement NIST SP 800-171 and the Framework.
Comprehensive (Y/N)	Yes
Reference Author	NIST
Reference Document Author	NIST
Comments	None
Point of Contact	Jane Doe 555-555-5555 example@nist.gov
Dependency/ Requirement	This Reference is a stand-alone Reference and does not have any dependencies.
Citations	None

Appendix E—Online CSF Informative Reference Participation Agreement

Online CSF Informative Reference Participation Agreement

This document establishes the terms of agreement for participating in the NIST Online CSF Informative References Program. Prior to submission of a candidate Informative Reference (Reference) to NIST, Reference submitters should ensure they have the most recent version of participation agreement document. The most recent version is available as a separate file at https://www.nist.gov/cyberframework.

National Institute of
Standards and Technology

Participation Agreement
The NIST CSF Online Informative References Program

Version 1.1
February 12, 2018

The phrase “NIST Online CSF Informative References Program” is intended for use in association with specific documents for which a candidate Informative Reference (Reference) has been created and has met the requirements of the Program for final listing on the submission on the Reference repository. You may participate in the Program if you agree in writing to the following terms and conditions:

1. References are made publicly available and free of charge.
2. You will follow expectations of the Program as outlined in the NIST Operational Procedures for the NIST Online CSF Informative References Program (https://www.nist.gov/cyberframework/reference-submission-page).
3. You will respond to comments and issues raised by a public review of your 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 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 Reference.
5. You will hold NIST harmless in any subsequent litigation involving the Reference submission.

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

7. You may not use the name 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 conditional on and limited to those References and the specific Reference versions for which a 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 conditional on and limited to those Reference submitters who provide assistance and help to users of the Reference with regard to proper use of the Reference and that the warranty for the Reference and the specific Reference versions is not changed by use of the 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 or regulatory reasons.

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

____

Organization or company name

____

Name and title of organization authorized person

____

Signature

____

Date