Withdrawn NIST Technical Series Publication

Warning Notice

The attached publication has been withdrawn (archived), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Withdrawn Publication	
Series/Number	NIST Internal Report 8204
Title	Cybersecurity Framework Online Informative References (OLIR) Submissions: Specification for Completing the OLIR Template
Publication Date(s)	April 2019
Withdrawal Date	May 31, 2019
Withdrawal Note	NISTIR 8204 is superseded in its entirety by the publication of NISTIR 8204 (includes updates as of May 31, 2019).

Superseding Publication(s) *(if applicable)*

The attached publication has been **superseded by** the following publication(s):

Series/Number	NIST Internal Report 8204
Title	Cybersecurity Framework Online Informative References (OLIR) Submissions: Specification for Completing the OLIR Template
Author(s)	Matthew Barrett; Nicole Keller; Stephen Quinn; Matthew Smith
Publication Date(s)	April 2019 (includes updates as of May 31, 2019)
URL/DOI	https://doi.org/10.6028/NIST.IR.8204

Additional Information *(if applicable)*

Contact	Applied Cybersecurity Division (Information Technology Laboratory)
Latest revision of the attached publication	
Related Information	https://www.nist.gov/cyberframework/informative-references https://csrc.nist.gov/publications/detail/nistir/8204/final
Withdrawal Announcement Link	

Date updated: May 31, 2019

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

NISTIR 8204

Cybersecurity Framework Online Informative References (OLIR) Submissions

Specification for Completing the OLIR Template

Matthew Barrett
Nicole Keller
Stephen Quinn
Matthew Smith

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8204

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

NISTIR 8204

Cybersecurity Framework Online Informative References (OLIR) Submissions

Specification for Completing the OLIR Template

Matthew Barrett*
Applied Cybersecurity Division
Information Technology Laboratory

Matthew Smith
G2, Inc.
Annapolis Junction, Maryland

Nicole Keller
Stephen Quinn
Computer Security Division
Information Technology Laboratory

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8204

April 2019

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
33 pages (April 2019)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8204

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

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 they complete 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.

Acknowledgments

The authors would like to thank Lisa Carnahan, Murugiah Souppaya, Vince Johnson, Jeff Marron, John Kelsey, 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.

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.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Informative Reference Development

This section describes the general process for developing Informative References ("References") and submitting them to the National Institute of Standards and Technology (NIST) for inclusion in the NIST Cybersecurity Framework's Online Informative Reference (OLIR) Catalog. It includes an overview of the process NIST will follow to screen the Informative Reference submissions and publish them in the OLIR Catalog on the Cybersecurity Framework's website [CSFweb].

Section 1 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 F. The agreement contains the administrative requirements for participating in the OLIR Program.

1.1 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 the Cybersecurity Framework. An Informative Reference shows the relationship(s) between the Reference Document elements and the Cybersecurity Framework elements. More exactly, Informative References show relationships between any number and combination of the Functions, Categories, and Subcategories of the Cybersecurity Framework and specific sections, sentences, or phrases of Reference Documents. The discrete Functions, Categories, Subcategories, and phrases of the Cybersecurity Framework, as well as specific sections, sentences, or phrases of the Reference Document shall be called Framework elements or Reference Document elements. The term 'Reference' or 'References' used in this document is an abbreviation for the term 'Informative Reference' or 'Informative References.'

1.2 Background

The *Framework for Improving Critical Infrastructure Cybersecurity* ("Cybersecurity Framework", "Framework") lists several related cybersecurity documents as Informative References [CSFv1.1]. 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 Online Informative References (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 to clearly define relationships between Reference Document elements and the Cybersecurity Framework elements.

1.3 Informative Reference Life Cycle

The Informative Reference life cycle comprises the following steps:

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

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

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

The first three steps in the development methodology listed above involve the developer creating, posting, and submitting Informative References. Sections 1.4.1 through 1.4.3 describe each of these steps in greater detail.

1.4.1 Initial Informative Reference Development

During initial Informative Reference development, a developer becomes familiar with the requirements of the OLIR Program and all procedures involved during the Informative Reference life cycle (as described throughout Section 1). At this point, a Developer would presumably agree to the requirements for participation in the OLIR Program before continuing to develop the Informative Reference. Appendix F of this publication provides the latest version of the Participation Agreement that SHALL be signed by the Developer.

The quality of Informative Reference documentation can significantly impact the Informative Reference's effectiveness. To promote consistency and facilitate the review of Informative References by NIST and the public, NIST has created a spreadsheet template ("OLIR Template").

Section 2 of this publication provides instructions and definitions for completing the OLIR Template.

1.4.2 Informative Reference Posting

Once the Informative Reference is implemented in the OLIR Template, the Developer SHALL post the Informative Reference to a public website. This posting enables NIST to link to the Informative Reference during both the comment period and the listing phase. The public website should be the same website as is listed in the *General Information* tab of the Informative Reference. The website listed in the OLIR Catalog can be updated if the Informative Reference's location changes. Section 2 also indicates that the Developer SHALL use the NIST-provided OLIR Validation tool to ensure that the populated OLIR Template conforms to the specifications in this publication.

1.4.3 Informative Reference Submitted to NIST

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

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

Submission packages are sent to the OLIR Program email alias, cyberframework-refs@nist.gov.

1.5 NIST Steps for Reviewing and Finalizing Informative References for Publication

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

1.5.1 NIST Screening of the Submission Package

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

1.5.2 Public Review and Feedback for the Candidate Informative Reference

After the submission package has been screened and the Developer has addressed any issues, NIST will post a link to the Informative Reference in the OLIR Catalog as a candidate in a 'draft' status for a 30-day public review period. NIST will invite the public to review and comment on the candidate Informative Reference and provide feedback to the Developer.[1]

[1] OLIR Catalog is located at https://www.nist.gov/cyberframework/reference-catalog.

An Informative 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 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; or
- NIST may disagree with the proposed issue resolutions and seek additional perspectives from third-party reviewers.

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

1.5.3 Final Listing in the OLIR Catalog

After any outstanding issues have been addressed, NIST will change the Informative Reference status to 'final' in the OLIR Catalog and will announce its availability. The listing will provide high-level data about the Informative Reference, including a link to the Informative Reference materials.

1.5.4 Informative Reference Maintenance and Archival

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

NIST will periodically review the catalog of Informative References to determine if individual Informative References are still relevant or if changes need to be made. If the Developer decides to update the Informative Reference at any time, NIST will announce that the Informative Reference is in the process of being updated and will reflect that in the OLIR Catalog listing. If the revised Informative Reference contains major changes (see Section 2.1.2 for version definitions), it will be considered as if it were a new submission and will be required to undergo the same review process as a new submission. If the Informative Reference contains minor changes, it will undergo a 30-day public comment period. If the Informative Reference contains administrative changes, no comment period is required, and the updated Informative Reference will be listed in the OLIR Catalog with an appropriate version number to annotate the update.

At NIST's or the Developer's discretion, the Informative Reference can either be archived or removed from the OLIR Catalog altogether. Typical reasons for such actions might be that the Reference Document is no longer supported or is obsolete, or the Developer no longer wishes to provide support for the Informative Reference. Unless otherwise requested by the Developer, withdrawn Informative References will be deleted from the OLIR Catalog and an entry will remain to indicate that an Informative Reference was previously available.

2 OLIR Template Instructions

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

2.1 Completing the General Information Tab

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

Table 1: General Information Tab Field Description

Field Name	Description
Informative Reference Name	The name by which the Informative Reference listing will be referred. The format is a human readable string of characters
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	URL where the Informative Reference can be found
Cybersecurity Framework Version	Framework version used in creating the Informative Reference. NIST recommends that Developers begin with Framework version 1.1 [CSFv1.1]. The version format is a string following the pattern: [major].[minor].[administrative]
Summary	The purpose of the Informative Reference
Target Audience (Community)	The intended audience for the Informative Reference
Comprehensive (Y/N)	Whether the Informative Reference maps *all* Reference Document elements to the Cybersecurity Framework document (“Yes”), or not (“No”)
Reference Document Author	The organization(s) and/or person(s) which published the Reference Document
Reference Document	Full Reference Document name and version that is being compared to the CSF
Reference Document Date	Date the Reference document was published and, if applicable, amended
Reference Document URL	Web address where the Reference Document can be viewed, downloaded, or purchased
Reference Developer	The organization(s) which created the Informative Reference
Comments	Notes to NIST or to implementers
Point of Contact	At least one person's name, email address, and phone number within the Informative Reference Developer organization
Dependency/ Requirement	Whether the Informative Reference is used in conjunction with other Informative Reference(s), or as a stand-alone Informative Reference

[2] The OLIR Template is a spreadsheet available at https://www.nist.gov/file/421906.

[3] The NISTIR 8204 OLIRVal tool is a .jar files that can be downloaded from https://www.nist.gov/cyberframework/online-informative-references-validation-tool

Field Name	Description
Citations	A listing of source material (beyond the Reference Document) which supported development of the Informative Reference

2.1.1 Informative Reference Name

In general, this field refers to the name of the spreadsheet mapping elements of the Reference Document to the Cybersecurity Framework. The name SHALL be human readable. The Informative Reference Name remains static over time.

Examples: "SP800-53-v4-to-CSF-v1-1"; "SP800-171-to-CSF-v1-1"

2.1.2 Reference Version

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

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

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

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

2.1.3 Web Address

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

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 [CSFv1.1].

Examples: "1.0"; "1.1".

2.1.5 Mapping Summary

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

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

2.1.6 Target Audience (Community)

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

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

2.1.7 Comprehensive

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

- "Yes": *all* Reference Document elements in the Reference Document are mapped to the Cybersecurity Framework document; otherwise,
- "No": one or more Reference Document elements in the Reference Document are *not* mapped to the Cybersecurity Framework document.

2.1.8 Reference Document Author

The Reference Document Author(s) refers to the organization(s) and/or person(s) who authored the Reference Document. For example, NIST is responsible for NIST SP 800-53 and would be listed as a Reference Document Author, even if a non-NIST Developer were to create an Informative Reference for [SP800-53]. Multiple authors SHALL be separated by commas.

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

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

2.1.9 Reference Document

A Reference Document is any cybersecurity document that is related to the Framework Core. This relationship SHOULD be defined at the Function, Category, and/or Subcategory levels of the Core.

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

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

2.1.10 Reference Document Date

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

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

2.1.11 Reference Document URL

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

2.1.12 Reference Developer

The Reference Developer is the author of the Informative Reference, and may be a person, team or organization. For example, a federal agency, product vendor or research academic may use a Reference Document (e.g., NIST Special Publication 800-53 [SP800-53]) and create an Informative Reference to the Cybersecurity Framework.

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

2.1.13 Comments

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

2.1.14 Point of Contact

The *Point of Contact* is a person associated with the Developer. The person named within this field SHOULD have subject matter expertise with the Informative Reference and be able to answer questions related to the Informative Reference. The format for this field is 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

2.1.15 Dependency/Requirement

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

2.1.16 Citations

The Citations field refers to documents that are supplementary to the Informative Reference. These documents may be standards or other supporting material 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

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

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, equal, 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 Reference Document element is part of a group of Reference Document elements that correlates to a Cybersecurity Framework Core element
Comments (optional)	Additional information useful to NIST or an implementer of the Informative Reference

The *Relationships* tab of the OLIR Template contains a row for each Function, Category, and Subcategory of the Cybersecurity Framework Core. The Developer 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 OLIR Template in this case.

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

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

2.2.1 Framework Element

The *Framework Element* refers to the Cybersecurity Framework Core element that is the target of the Reference Document mapping. In the OLIR Template, the *Relationships* tab includes a row for every Framework element, where Function, Category, and Subcategory are represented. These rows are provided for convenience only. If a Reference Document has multiple mappings to the same Framework element, the Developer SHALL include additional rows. Rows that are deemed unnecessary by the Developer SHALL remain blank. The format of these fields corresponds to the Cybersecurity Framework Core element identifiers found in Table 2 of the Cybersecurity Framework source document (e.g., [CSFv1.1]).

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

2.2.2 Framework Element Description

The *Framework Element Description* refers to the text description of the Cybersecurity Framework Core element. This description is a fixed value that is included here for convenience and readability. The Developer shall copy this text if additional rows are necessary.

Examples: Data at rest is protected; impact of events is determined.

2.2.3 Rationale

The explanation of why a given Reference Document element and Framework element are related is attributed to one of three basic reasons. In Section 2.2.4 and Appendix F, these are referred to as the "logical comparison approaches".

Syntactic – Analyzes the linguistic meaning of the Reference Document element and Framework element to develop the conceptual comparison sets. Syntactic analysis uses literal analysis of (i.e., translates) the Reference Document or Framework elements.

> *Example 1*: A syntactic mapping might be established between the phrases "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 Reference Document element and Framework element to develop the conceptual comparison sets. Semantic analysis interprets (i.e., transliterates) the language within the Reference Document or Framework elements

Example 1: A semantic mapping might be established between the phrases “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 (i.e., transposes) the functions of the Reference Document element and Framework element to develop the conceptual comparison sets.

Example 1: A functional mapping might be established between the phrases “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 Developer SHALL populate the corresponding *Rationale* field with one of the three explanations above: *syntactic*, *semantic*, or *functional*.

2.2.4 Relationship

The *Relationship* field refers to the logical comparison between Reference Document elements and the Framework elements. When read left to right, a relationship represents a one-way mapping from the Reference Document to the Framework. While this may seem counterintuitive for the Developer, it results in an Informative Reference that is more user-friendly and consumable.

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

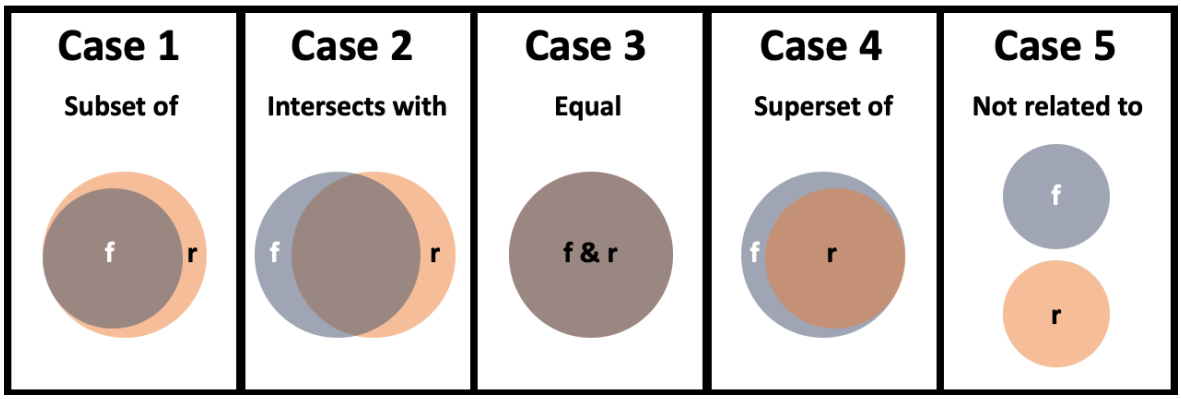

Figure 1: Informative Reference Relationship Types
(f = Framework element concept(s); r = Reference Document element concept(s))

A relationship SHALL be determined using one or more rationales defined in section 2.2.3. 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.

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

2.2.5 Reference Document Element

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

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

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

In the instance of creating identifiers, Developers SHALL clearly identify which sections of text are being related to the Framework element as described in Section 2.2.6. In other words, the Reference Document Element Description becomes a mandatory field.

Examples:

> Pertaining to [ISO27001]:
>
> > [A.6.3] - Designates A.6.3 as the Reference Document element being mapped
>
> Pertaining to [SP800-53]:

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

The Informative Reference SHALL focus on the main intuitive topic of the Reference Document and Framework elements being compared. If a Reference Document Element contains more than one main topic, the Developer SHALL decompose it into multiple, discrete Reference Document elements. In this instance, the Developer SHALL use additional Sequential Identifiers to clearly identify which sections of text are being related to the Framework element as described in Section 2.2.8; also, the Reference Document Element Description becomes a mandatory field. The Developer SHALL use the following format when creating identifiers:

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

Examples:

Pertaining to [ISO27001]:

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

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

Pertaining to [SP800-53]:

[AC-13:3] - Designates the 3rd portion of 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 Reference Document Element Description

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

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

2.2.7 Fulfilled By

The *Fulfilled By* field refers to the completeness of a Reference Document element in relation to a Framework element. Framework elements that are subsets of or equal to Reference Document elements SHALL 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 2.2.8), the appropriate Yes/No value is selected relative to the entire group, instead of the individual Reference Document element. In these

cases, the *Fulfilled By* value for each Reference Document element SHALL be the same as the collective Group value.

2.2.8 (Optional) Group Identifier

The *Group identifier* is a value defined by the Developer. This value indicates that individual Reference Document elements are part of a group when mapped to a Framework element. The Developer SHOULD create a Group Identifier to indicate that a group of Reference Document elements fulfill a Framework 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 to any Function, Category, or Subcategory. The Group Sequential Identifier is the literal "G" followed by the sequential number which designates the position of the group. Examples:

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

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

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

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

Note that only one colon (":") may be used in the identifier, specifically to separate the Reference Document Element from the Group Sequential Identifier. See Table 3 in Section 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 Informative Reference consumers understand the developer's logic. The Developer may wish to provide additional information to Informative Reference users to explain decisions made or implementation considerations.

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 Developer; they 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 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 By* column is marked "No" for all rows.

Table 3: Template Examples for Multiple Reference Document Elements

Framework Element	Framework Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	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 equal to a Reference Document element. This Relationship designation indicates that the Reference Document element entirely fulfills the Category.

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

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

Appendix A—Relationship Examples

The logic for determining the relationships depicted in Figure 1 is presented below:

$$Where\ F\ is\ the\ set\ of\ all\ Framework\ elements\ and\ R\ is\ the\ set\ of\ all\ Reference\ Document\ elements;$$

$$Where\ f\ is\ a\ Framework\ element;$$

$$Where\ r\ is\ a\ Reference\ Document\ element;$$

$$Where\ m_1\ or\ m_2\ represent\ functions\ which\ produce\ concept\ sets;$$

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

$$Reference\ Document\ element\ concepts = C_r = \{m_2(r) \mid r \in R\}$$

$$Shared\ concepts = C_S = C_f \cap C_r$$

The examples below are extended explanations of the Relationships described in Section 2.2.4. The examples were taken from NIST SP 800-171, and all Reference Document elements are referenced as described in that publication [SP800-171]; all Framework element examples are taken from version 1.1 of the Cybersecurity Framework [CSFv1.1].

Case 1 – Subset of

In Figure 1, the Venn Diagram in 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: [SP800-171] 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 Developer is using a *functional* mapping technique as described in Section 2.2.3. PR.AT-4 states that a specific group of users (Senior executives) should be trained on their roles and responsibilities. Requirement 3.2.2 in [SP800-171] states that "all users" should be trained on their roles and responsibilities. The concept "all users" contains the concept "Senior executives and others."

Given that

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

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

"[CSFv1.1] element PR.AT-4 is a subset of [SP800-171] requirement 3.2.2."

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 Reference Document element and Framework element share concepts.

$$If\ C_f - C_S \neq\ \emptyset\ \ and\ \ \ C_r - C_S \neq \emptyset, then\ Relationship = "intersects\ with"$$

Example

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

Reference Document element: [SP800-171] requirement 3.6.2, "Track, document, and report incidents to appropriate organizational officials and/or authorities."

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

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

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

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

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

If the Developer uses a *syntactic* mapping technique as described in Section 2.2.3, the shared concepts are "incidents" and "reporting." However, RS.CO-2 contains the concept of "established criteria" and [SP800-171] requirement 3.6.2 contains the concepts of "track," "document," "appropriate organizational officials," and "authorities."

Given that the compared Reference Document element and Framework element

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

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

"[CSFv1.1] element RS.CO-2 intersects with [SP800-171] requirement 3.6.2."

Case 3 – Equal

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, and neither the Reference Document nor the Framework element has any unique concepts.

$$If\ C_S = C_f = C_r, then\ Relationship = "equal\ to"$$

Example

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

Reference Document element: [SP800-171] requirement 3.4.6, "Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities."

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

$$C_r = m(3.4.6) = \begin{Bmatrix} principle\ of\ least\ functionality, \\ configuring\ systems, \\ provide\ essential\ capabilities \end{Bmatrix}$$

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

$$C_S = C_f = C_r \rightarrow "Equal\ to"$$

If the Developer uses either a *functional* or *semantic* mapping technique as described in Section 2.2.3, the shared concepts are "principle of least functionality," "configuring systems," and "provide essential capabilities." Neither the Reference Document element nor the Framework element contains any unique concepts.

Given that the Reference Document element and Framework element

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

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

"[CSFv1.1] element PR.PT-3 is equal to [SP800-171] requirement 3.4.6."

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.

$$If\ C_S = C_r\ \ and\ C_f - C_S \neq \emptyset, then\ Relationship = "superset\ of"$$

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: [SP800-171] requirement 3.5.1 Identify system users, processes acting on behalf of users, and devices.

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

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

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

$$C_S = C_r$$

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

If the Developer uses a *functional* mapping technique as described in Section 2.2.3, to issue a credential, a process or user would have to be identified. While [SP800-171] requirement 3.5.1 contains this identification, the management, verification, revocation, and audit of the credential is also contained in the Framework element.

Given that

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

their designated relationship is “superset of.” In other words,

“[CSFv1.1] element PR.AC-1 is a superset of [SP800-171] requirement 3.5.1.”

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, so the former may be omitted or marked "Not related to", along with a blank Framework Element field. If a Reference Document element is omitted entirely from the OLIR Template, it will be assumed to be "not related to" any Framework element.

$$If\ C_S = \emptyset, then\ Relationship = "Not\ Related\ to".$$

Appendix B—Acronyms

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

CSF	Cybersecurity Framework
DE	Detect
DE.AE	Detect, Anomalies and Events
DHS	Department of Homeland Security
HIPAA	Health Insurance Portability and Accountability Act
ID	Identify
ITL	Information Technology Laboratory
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
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
RC	Recover
RC.CO	Recover, Communications
RS	Respond
RS.CO	Respond, Communications
SP	Special Publication
URL	Uniform Resource Locator

Appendix C—Glossary

Developer	A person, team, or organization that creates an Informative Reference.
Informative Reference (Reference)	A relationship between a Reference Document and the NIST Cybersecurity Framework, using the OLIR Template.
OLIR Catalog	The Online Informative References (OLIR) Catalog, which provides information about the Informative References submitted to and accepted by NIST.
OLIR Program	NIST's Cybersecurity Framework (CSF) Online Informative References Program
OLIR Template	A spreadsheet that contains the fields necessary for creating a well-formed Informative Reference for submission to the OLIR Program. It is available on the Cybersecurity Framework website and serves as the starting point for the Developer.
Reference Document	A cybersecurity document that is related to the Framework.

Appendix D—Bibliography

[CSFv1.1] National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1 (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

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

[ISO27001] 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

[RFC2119] 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

[SP800-53] 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

[SP800-171] Ross R, Dempsey K, Viscuso P, Riddle M, Guissanie G (2016) *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171 Rev. 1, Includes updates as of June 7, 2018. https://doi.org/10.6028/NIST.SP.800-171r1

Appendix E—General Information Example

The table below displays field values that adhere to the specification within Section 2.1.

Field Name	Field Value
Informative Reference Name	NIST SP 800-171 Reference
Reference Version	1.0.0
Web Address	http://www.nist.gov/files/xxxxxx
Cybersecurity Framework Version	1.1
Mapping Summary	The purpose of this Informative Reference is to provide a relationship between the NIST SP 800-171 document and the Framework.
Target Audience (Community)	The intended audience for this Informative Reference is those seeking to protect controlled unclassified information using the Framework.
Comprehensive (Y/N)	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 555-555-5555 example@nist.gov
Dependency/ Requirement	This Informative Reference is a stand-alone Reference and does not have any dependencies.
Citations	Mapping of Cybersecurity Framework v.1.0 to SP 800 171 Rev. 1, https://csrc.nist.gov/CSRC/media//Publications/sp/800-171/rev-1/final/documents/csf-v1-0-to-sp800-171rev1-mapping.xlsx

Appendix F—Participation Agreement for the NIST CSF OLIR Program

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

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 Informative Reference repository. You may participate in the Program if you agree in writing to the following terms and conditions:

1. Informative References are made reasonably available.
2. You will follow expectations of the Program as detailed in the NIST Interagency Report 8204 Section 1.
3. You will respond to comments and issues raised by a public review of your Informative Reference submission within 30 days of the end of the public review period. Any comments from reviewers and your responses may be made publicly available.
4. You agree to maintain the Informative Reference and provide a timely response (within 10 business days) to requests from NIST for information or assistance regarding the contents or structure of the Informative Reference.
5. You represent that, to the best of your knowledge, the use of your Informative Reference submission will not infringe any intellectual property or proprietary rights of third parties. You will hold NIST harmless in any subsequent litigation involving the Informative Reference submission.
6. You may terminate your participation in the Program at any time. You will provide two business weeks' notice to NIST of your intention to terminate participation. NIST may

terminate its consideration of Informative 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 convincing supporting evidence to rebut that termination.

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

By 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