Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date August 4, 2020

Original Release Date January 24, 2020

Superseding Document

Status	2nd Public Draft (2PD)
Series/Number	NIST Interagency or Internal Report 8278
Title	National Cybersecurity Online Informative References (OLIR) Program: Program Overview and OLIR Uses
Publication Date	August 2020
DOI	https://doi.org/10.6028/NIST.IR.8278-draft2
CSRC URL	https://csrc.nist.gov/publications/detail/nistir/8278/draft
Additional Information	

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

Draft NISTIR 8278

National Cybersecurity Online Informative References (OLIR) Program:

Guidance for OLIR Users and Developers

Nicole Keller
Stephen Quinn
Karen Scarfone
Matthew Smith
Vincent Johnson

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

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

Draft NISTIR 8278

National Cybersecurity Online Informative References (OLIR) Program:

Guidance for OLIR Users and Developers

Nicole Keller
Stephen Quinn
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

Matthew Smith
Huntington Ingalls Industries
Annapolis Junction, MD

Vincent Johnson
Electrosoft Services, Inc.
Reston, VA

January 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8278
30 pages (January 2020)

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

Public comment period: *January 24, 2020* through *February 24, 2020*

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

77 ## Reports on Computer Systems Technology

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

86 ## Abstract

87 In a general sense, an informative reference indicates how one document relates to another
88 document. The National Cybersecurity Online Informative References (OLIR) Program is a
89 NIST effort to facilitate subject matter experts defining standardized online informative
90 references (OLIRs) between elements of their documents and elements of other documents like
91 the NIST Cybersecurity Framework. The OLIR Program provides a standard format for
92 expressing OLIRs and a centralized location for hosting them. This report describes the OLIR
93 Program, focusing on explaining what OLIRs are and what benefits they provide, how anyone
94 can search and access OLIRs, and how subject matter experts can contribute OLIRs.

95 ## Keywords

96 catalog; Cybersecurity Framework; informative references; mapping; Online Informative
97 References (OLIRs).

98

Acknowledgments

The authors—Nicole Keller and Stephen Quinn of NIST, Karen Scarfone of Scarfone Cybersecurity, Matthew Smith of Huntington Ingalls Industries, and Vincent Johnson of Electrosoft Services Inc.—wish to thank all individuals and organizations who contributed to the creation of this document. Contributors include Murugiah Souppaya, Robert Byers, Eduardo Takamura, Vicky Pillitteri, and Kevin Stine of NIST; Alex Jordan, Information Security Forum; Dr. Bryan Cline, HITRUST Alliance, LLC; Dr. Jack Freund, RiskLens; Joshua Franklin, Center for Internet Security; Christian Nickel, Huntington Ingalls Industries; Anca Sailer, IBM; Amrita Satapathy and Becky Ochs, Microsoft; and Tarik Williams, RSA.

Audience

Consumers who might benefit most from this publication include cybersecurity subject matter experts, framework developers and consumers, cybersecurity professionals, auditors, and compliance specialists.

Trademark Information

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: cyberframework-refs@nist.gov

Executive Summary

The fields of cybersecurity, privacy, and workforce have a large number of documents, such as standards, guidance, and regulations. There is no standardized way to indicate how an element of one document relates to an element of another document—for example, the relationship between requirement A in one document and recommendation 7.2 in another document. This relationship is called an *informative reference*. The *Framework for Improving Critical Infrastructure Cybersecurity* ("Cybersecurity Framework") [1] introduced informative references, but these were simple prose mappings that only noted a relationship existed, and not the nature of that relationship. Also, these informative references were part of the Cybersecurity Framework document itself, so they could not readily be updated as the other documents in the relationships changed.

The National Cybersecurity Online Informative References Program is a NIST effort to facilitate subject matter experts (SMEs) defining standardized online informative references (OLIRs) between elements of their cybersecurity, privacy, and workforce documents and elements of other cybersecurity, privacy, and workforce documents like the Cybersecurity Framework. At this stage of the OLIR Program evolution, the initial focus is relationships to cybersecurity documents. The OLIRs are in a simple standard format defined by NIST Interagency Report (IR) 8204, *Cybersecurity Framework Online Informative References (OLIR) Submissions: Specification for Completing the OLIR Template* ("NISTIR 8204") [2], and they are hosted in a centralized repository. By following this approach, cybersecurity document owners can use the OLIR Program as a mechanism for communicating with owners and users of other cybersecurity documents.

The OLIR Program integrates ongoing NIST projects that respond to administrative and legislative requirements, including those for the Cybersecurity Framework under Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, [3] released in February 2013, and the Federal Information Security Modernization Act of 2014 [4], which amended the Federal Information Security Management Act of 2002 (FISMA). Also addressed by the OLIR Program are many Office of Management and Budget (OMB) memoranda that address specific cybersecurity issues and comprise large sets of regulations to which organizations must track and comply. The OLIR Program can incorporate any authoritative documents, from national and international standards, guidelines, frameworks, and regulations to policies for individual organizations, sectors, or jurisdictions.

The purpose of this document is to describe the National Cybersecurity OLIR Program and explain the use, benefits, and management of the OLIR Catalog—the online repository for hosting and sharing OLIRs—for both the SMEs contributing OLIRs to it and the Catalog's users. The contents of this document complement those of NISTIR 8204. [2]

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

1.1 Purpose and Scope

The purpose of this document is to describe the National Cybersecurity Online Informative References (OLIR) Program and explain the use, benefits, and management of the OLIR Catalog for Informative Reference Developers ("Developers") and Informative Reference Users ("Users") of the OLIR Program.

1.2 Document Structure

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

- Section 2 provides an overview of the OLIR Program.
- Section 3 describes common uses of the OLIR Catalog relevant to both Developers and Users.
- Section 4 offers additional information on the OLIR Program for Developers that supplements the material in Section 3.
- The References section lists the references for the publication.
- Appendix A contains acronyms used throughout the document.
- Appendix B provides a glossary of terminology used throughout the document.
- Appendix C includes the Participation Agreement for the OLIR Program for Developers.

2 Overview of the National Cybersecurity OLIR Program

In a general sense, an informative reference, also called a mapping, indicates how one document relates to another document. Within the context of the National Cybersecurity OLIR Program, an *Informative Reference* (abbreviated as *Reference)* indicates the relationship(s) between elements of two documents. Although using Informative References can significantly improve understanding within organizations, using an Informative Reference cannot demonstrate or certify that an organization complies with a document. The source document, called the *Focal Document*, is used as the basis for the document comparison. The second document is called the *Reference Document*. Note that a Focal Document or a Reference Document is not necessarily in a traditional document format—it could be a product, service, training, etc. A *Focal Document element* or a *Reference Document element* is a discrete section, sentence, phrase, or other identifiable piece of content of a document.

As of this writing, the OLIR Program has a single Focal Document: the *Framework for Improving Critical Infrastructure Cybersecurity* ("Cybersecurity Framework") version 1.1 [1]. Informative References were originally documented within the Cybersecurity Framework document. While the concept of References was well received, the static nature of the Cybersecurity Framework document meant that some of its References became outdated as Reference Documents were updated. For example, in version 1.1 of the Cybersecurity Framework, the PR.DS-1 Subcategory, "Data-at-rest is protected" had References to controls from the Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense. CIS published a new version of their controls as the Cybersecurity Framework version 1.1 was being finalized, and since that time CIS has published another new version, but it is not practical to update the Cybersecurity Framework every time a Reference Document is updated.

The OLIR Program provides an online repository, the OLIR Catalog, for hosting, sharing, and comparing References. The OLIR Program defines a simple format in NISTIR 8204 [2] for expressing References in the OLIR Catalog in a standardized, consistent manner. This offers several benefits, including the following:

- There are many potential Reference Documents, so the OLIR Program provides a single easy-to-use place where people can get information on many Reference Documents and analyze their relationships. This also significantly reduces the time organizations need to research and analyze their current and target cybersecurity activities, and to communicate with others regarding cybersecurity activities. Without a central repository, finding and comparing cybersecurity resources can be difficult. Also, it may be difficult to determine if a cybersecurity resource is current or how the resource should be used.
- The OLIR Program increases transparency, alignment, and harmonization of definitions and concepts across Reference Documents.
- Standardizing how References are expressed makes them more consistent, clear, usable, repeatable, and organizable, and it provides a way for automation technologies to ingest and utilize them.

- Having a centralized OLIR Program enables authenticating the source of each Reference and tagging each Reference as coming from a verified subject matter expert (SME) on the Reference Document or from someone else.
- The OLIR Program employs additional mathematic rigor—including standard set theory principles, such as subset, superset, equal, and intersect, and discrete logic—to express References instead of using prose, which is ambiguous and subject to individual interpretation.
- The OLIR Program increases integration of NIST guidance produced in support of United States Government (USG) legislative and administrative responsibilities.

The OLIR Program also defines a formal process for vendors and other OLIR Developers to submit OLIRs to NIST. This process includes guidance to Developers on creating high-quality, more usable, better documented OLIRs. It also defines a managed process for the review, update, and maintenance of OLIRs as Focal and Reference Documents are updated and revised.

3 Common Uses of the OLIR Catalog

This section provides information on use of the OLIR Catalog for both OLIR Developers and Users. Section 3.1 explains the types of information the Catalog contains. Section 3.2 reviews the interfaces for viewing and searching the OLIRs in the Catalog, as well as the supporting information the Catalog holds for each OLIR. Section 3.3 provides information on an analysis tool that helps characterize relationships among Reference Documents. Section 3.4 explains how to generate comparative analysis reports between OLIRs at different levels of abstraction, and Section 3.5 discusses how to download reports. Finally, Section 3.6 talks about use cases for the OLIR Catalog.

3.1 Reference Data

The OLIR Catalog contains two types of information on the relationships between Focal Documents and Reference Documents: Informative References and Derived Relationship Mappings. These relationships are organized as *Reference Data* via the OLIR Catalog according to the vetting processes delineated in NISTIR 8204, with the objective of providing transparency from the Informative Reference Developers for reproducibility and discussion by Users.

3.1.1 Tier 1 – Informative References

Tier 1 Reference Data are Informative References that have been vetted with respect to NIST documents by NIST staff, submitted for a public comment period, and finalized. The OLIR Program has two major groups of References:

- **Owner:** These are produced by the owner of the Reference Document. For example, NIST is the owner of NIST Special Publication (SP) 800-171 and produced the Informative Reference for SP 800-171; therefore, the designation of "owner" is granted to the SP 800-171 Informative Reference developed by NIST.
- **Non-Owner:** These are produced by anyone who is NOT the Reference Document owner. For example, if Organization A developed an Informative Reference for SP 800-171, the Informative Reference would be designated "non-owner."

Reference Document owners who create Informative References will not only provide more consistency in cybersecurity communication among federal agencies, but also provide a much more cost-effective method for establishing and verifying the relationships between Reference Documents through Focal Documents. NIST encourages Reference Document owners, software vendors, service providers, educators, and other parties to develop and submit References to the OLIR Program.

When multiple Informative References are available for a particular Reference Document, Users should take into consideration the sources of the Informative References. Generally, Informative References from owners can be used more consistently and efficiently than Informative References from non-owners. If it is not clear which Informative Reference should be analyzed based on the authority of the submission (owner/non-owner), then Users should focus on the quality and completeness of the Informative Reference Developer.

3.1.2 Tier 2 – Derived Relationship Mappings (DRMs)

Tier 2 Reference Data are the Derived Relationship Mappings (DRMs). DRMs are the result of analyzing Reference Documents related to the Focal Document and using those relationships to make inferences about document-to-document relationships. Figure 1 depicts how someone could find the relationship between Reference Document 1 Element A and Reference Document 2 Element B based on their individual relationships to Focal Document Element E. DRMs are dynamically generated when someone uses the DRM Analysis Tool to search the OLIR Catalog on the OLIR website, as described in Section 3.3. The results of the search are displayed to the user as shown in Figure 6. DRMs serve as the foundation for gap and comparative analysis.

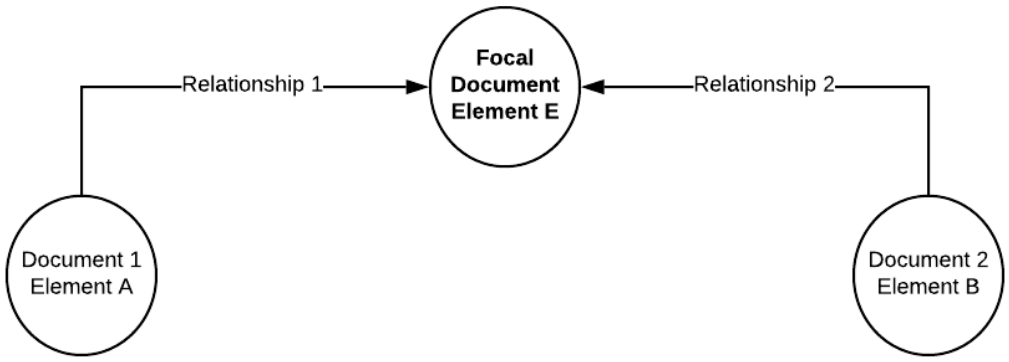


Figure 1: Multiple Documents Related to a Focal Document

While the inferences a User makes about DRMs are informative, they are not considered verified nor authoritative. DRMs help users of cybersecurity documents to make informed decisions regarding cybersecurity risk management activities. See Section 3.6 for common use cases.

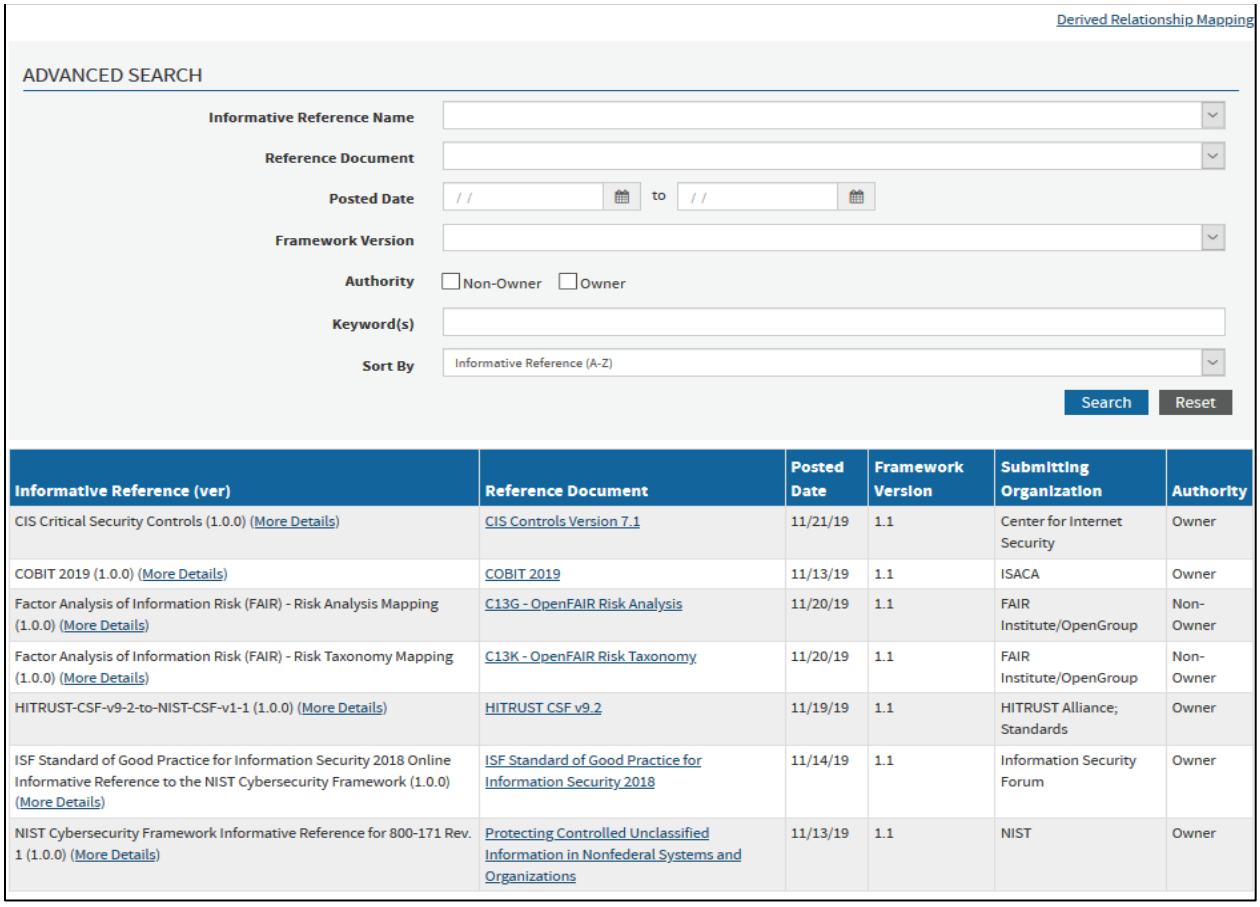
3.2 The OLIR Catalog

The OLIR Catalog (https://csrc.nist.gov/Projects/Cybersecurity-Framework/Informative-Reference-Catalog) contains all the Reference Data—Informative References and DRMs—for the National Cybersecurity OLIR Program. All Reference Data in the OLIR Catalog has been validated against the requirements of NISTIR 8204. The OLIR Catalog provides interfaces for Developers to submit Informative References and for Users to view and analyze Reference Data.

The Catalog includes links to draft content that is being evaluated during a 30-day public comment period and final versions that have completed the public comment period. Following the public comment adjudication period, draft content is replaced with the final version, and the draft content is removed from the catalog.

Figure 2 shows the OLIR Catalog Page. From this page, Users can browse Informative Reference descriptions to locate and retrieve an Informative Reference using a variety of fields, such as Informative Reference (name), Reference Document, Framework Version, Submitting Organization, and Authority. Users can also browse and search Informative Reference content in multiple ways. Using dropdowns in the *Advanced Search* section, Users can search for content

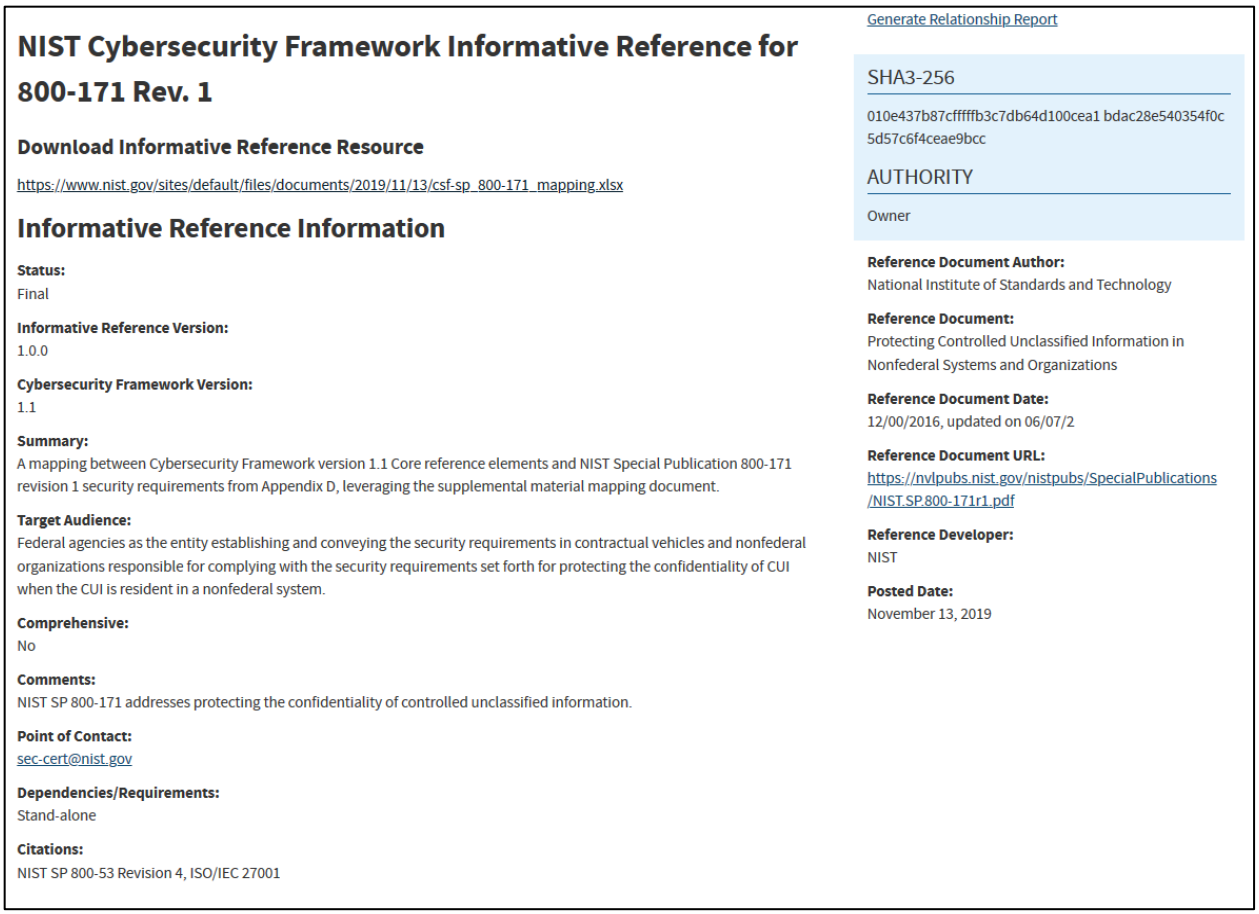
by the Informative Reference Name, Reference Document, and Cybersecurity Framework version. Users can also perform keyword searches of Catalog content and can sort the catalog columns within the table either alphabetically (A-Z) or numerically by the Posted Date that a submission was added to the Catalog.



Informative Reference (ver)	Reference Document	Posted Date	Framework Version	Submitting Organization	Authority
CIS Critical Security Controls (1.0.0) (More Details)	CIS Controls Version 7.1	11/21/19	1.1	Center for Internet Security	Owner
COBIT 2019 (1.0.0) (More Details)	COBIT 2019	11/13/19	1.1	ISACA	Owner
Factor Analysis of Information Risk (FAIR) - Risk Analysis Mapping (1.0.0) (More Details)	C13G - OpenFAIR Risk Analysis	11/20/19	1.1	FAIR Institute/OpenGroup	Non-Owner
Factor Analysis of Information Risk (FAIR) - Risk Taxonomy Mapping (1.0.0) (More Details)	C13K - OpenFAIR Risk Taxonomy	11/20/19	1.1	FAIR Institute/OpenGroup	Non-Owner
HITRUST-CSF-v9-2-to-NIST-CSF-v1-1 (1.0.0) (More Details)	HITRUST CSF v9.2	11/19/19	1.1	HITRUST Alliance; Standards	Owner
ISF Standard of Good Practice for Information Security 2018 Online Informative Reference to the NIST Cybersecurity Framework (1.0.0) (More Details)	ISF Standard of Good Practice for Information Security 2018	11/14/19	1.1	Information Security Forum	Owner
NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1 (1.0.0) (More Details)	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	11/13/19	1.1	NIST	Owner

Figure 2: OLIR Catalog Page

Selecting the "More Details" link of an Informative Reference in the Catalog will display a description page, shown in Figure 3, that includes the General Information of an Informative Reference as provided by the Developer.



NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1

Download Informative Reference Resource

https://www.nist.gov/sites/default/files/documents/2019/11/13/csf-sp_800-171_mapping.xlsx

Informative Reference Information

Status:
Final

Informative Reference Version:
1.0.0

Cybersecurity Framework Version:
1.1

Summary:
A mapping between Cybersecurity Framework version 1.1 Core reference elements and NIST Special Publication 800-171 revision 1 security requirements from Appendix D, leveraging the supplemental material mapping document.

Target Audience:
Federal agencies as the entity establishing and conveying the security requirements in contractual vehicles and nonfederal organizations responsible for complying with the security requirements set forth for protecting the confidentiality of CUI when the CUI is resident in a nonfederal system.

Comprehensive:
No

Comments:
NIST SP 800-171 addresses protecting the confidentiality of controlled unclassified information.

Point of Contact:
sec-cert@nist.gov

Dependencies/Requirements:
Stand-alone

Citations:
NIST SP 800-53 Revision 4, ISO/IEC 27001

Generate Relationship Report

SHA3-256

010e437b87cfffffb3c7db64d100cea1 bdac28e540354f0c5d57c6f4ceae9bcc

AUTHORITY

Owner

Reference Document Author:
National Institute of Standards and Technology

Reference Document:
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Reference Document Date:
12/00/2016, updated on 06/07/2

Reference Document URL:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

Reference Developer:
NIST

Posted Date:
November 13, 2019

Figure 3: Informative Reference More Details Page

Table 1 lists fields and descriptions of the information depicted on the More Details page in Figure 3.

Table 1: Informative Reference More Details Description Fields

Field Name	Description
Informative Reference Name	The name by which the Informative Reference listing will be known. The format is a human-readable string of characters.
Web Address	The URL where the Informative Reference can be found
Status	Indicates if an Informative Reference is in “Draft” (not yet final) or “Final” (after the comments from the public comment period have been addressed)
Informative Reference Version	The version of the Informative Reference itself. The format is a string following the pattern: [major].[minor].[administrative]. The initial submission has an Informative Reference Version of 1.0.0.
Cybersecurity Framework Version	The Cybersecurity Framework version used in creating the Informative Reference. NIST recommends that Developers begin with version 1.1.[1]

[1] This field will be modified as additional Focal Documents are added to the OLIR Program.

Field Name	Description
Summary	The purpose of the Informative Reference
Target Audience	The intended audience for the Informative Reference
Comprehensive	Whether the Informative Reference maps *all* Reference Document elements to the Focal Document ("Yes") or not ("No")
Comments	Notes to NIST or implementers
Point of Contact	At least one person's name, email address, and phone number within the Informative Reference Developer organization
Dependencies/Requirements	Whether the Informative Reference is used in conjunction with other Informative Reference(s), or as a standalone Informative Reference
Citations	A listing of source material (beyond the Reference Document) that supported development of the Informative Reference
SHA3-256	The hash value checksum that is generated between the validated Informative Reference sent to the OLIR Program and the publicly available hosted Informative Reference. The value is monitored to maintain data integrity of the hosted Informative Reference.
Authority	The organization responsible for authoring the Informative Reference in relation to the organization that produced the Reference Document represented by the Informative Reference submission
Reference Document Author	The organization(s) and/or person(s) that published the Reference Document
Reference Document	The full Reference Document name and version that is being compared to the Focal Document
Reference Document Date	The date the Reference Document was published and, if applicable, amended
Reference Document URL	The URL where the Reference Document can be viewed, downloaded, or purchased
Reference Developer	The organization(s) that created the Informative Reference
Posted Date	The date that a validated Informative Reference submission was added to the catalog for the draft public comment period or final posting following the completion of the public comment period and adjudication process

3.3 The DRM Analysis Tool

The DRM Analysis Tool (https://csrc.nist.gov/Projects/Cybersecurity-Framework/Derived-Relationship-Mapping) provides Users the ability to generate DRMs for Reference Documents with the Cybersecurity Framework as the Focal Document. The DRMs are non-authoritative and represent a starting point when attempting to compare Reference Documents. Figure 4 depicts the home page of the DRM Analysis Tool.

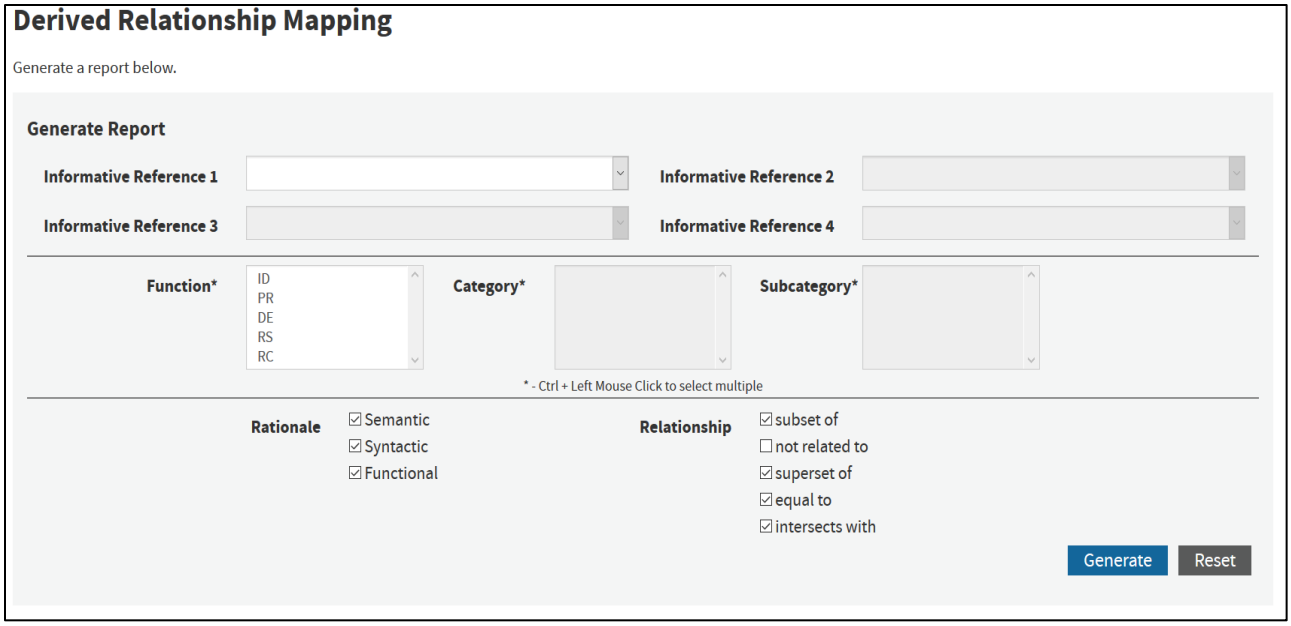
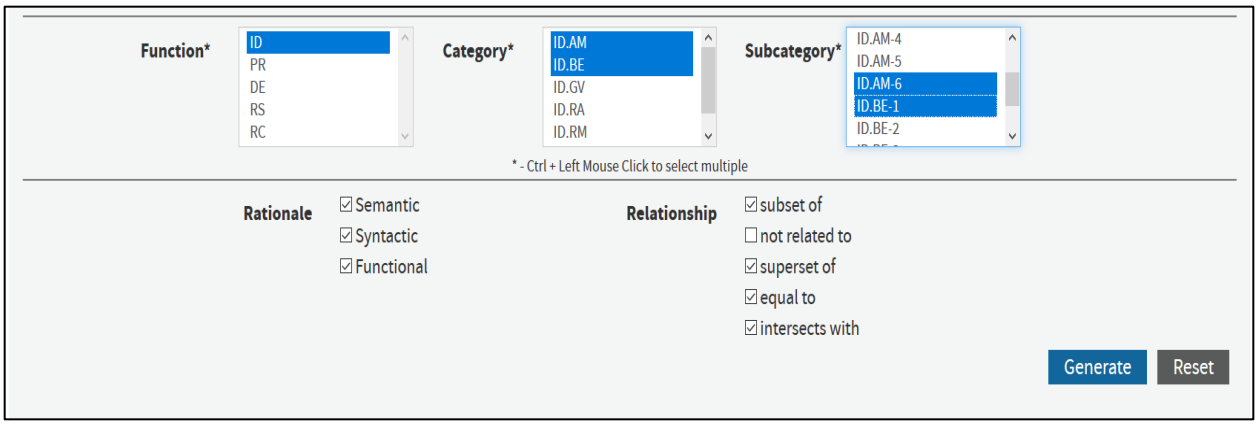


Figure 4: DRM Analysis Tool Home Page

As Figure 4 shows, when accessing the DRM Analysis tool, Users have the ability to compare up to four Informative References at a time. Users can generate reports at any level (Function, Category, Subcategory) of the Cybersecurity Framework. When a User accesses this page, by default all rationale and relationships pairings (except the "not related to" relationship) are pre-selected. To filter out any rationale or relationship selections, the User can de-select a checkbox as appropriate before generating a report.

In addition to performing an analysis at an individual level (i.e., selecting one Function, Category, or Subcategory), Users have the ability to compare Informative References at multiple levels (i.e., selecting multiple Functions, Categories, and Subcategories). Figure 5 displays an example of multiple Categories and Subcategories marked as selected for analysis. In this example, the two Categories being analyzed are ID.AM and ID.BE along with Subcategories ID.AM-6 and ID.BE-1. To achieve this desired analysis, a User should first select the 'ID' Function, which will result in the applicable Categories being displayed in the Category box. To select multiple Categories, the user can hold the "ctrl" key on a Windows computer and click on the ID.AM and ID.BE Categories. On a macOS computer, the user should hold the "command" key instead of the "control" key. Choosing both ID.AM and ID.BE will cause all of the Subcategories within ID.AM and ID.BE to be displayed in the Subcategory box. Users can continue this selection behavior to select multiple Subcategories.



411

412 **Figure 5: Multi-Select Example**

413 ## 3.4 Display Report

414 After selecting the 'Generate' option (see Figure 5), Users are presented with an on-screen
415 output table. Figure 6 shows the results from comparing two particular Informative References at
416 the individual PR.AC-2 Subcategory level. This on-screen output is the *Display Report*.

Function(s): PR **Category(s):** PR.AC **Subcategory(s):** PR.AC-2
Rationale(s): Semantic, Syntactic, Functional
Relationship(s): subset of, superset of, equal to, intersects with

Framework Element	Informative Reference Name	Reference Document Element	Rationale	Relationship	Reference Element Description	Comments	Group
PR.AC-2	NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1	3.10.1	Semantic	superset of	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	Limiting access is a form of protection, but it needs to be monitored (managed).	
PR.AC-2	NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1	3.10.2	Semantic	intersects with	Protect and monitor the physical facility and support infrastructure for organizational systems.		
PR.AC-2	NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1	3.10.3	Functional	intersects with	Escort visitors and monitor visitor activity.		
PR.AC-2	NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1	3.10.4	Functional	intersects with	Maintain audit logs of physical access.		
PR.AC-2	NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1	3.10.5	Functional	superset of	Control and manage physical access devices.	"Physical access devices" may be considered "assets."	

417

418 **Figure 6: Display Report Example**

419 **Understanding Section 3.1.2 of this document is a prerequisite to understanding the**
420 **Display Report**. Due to screen space limitations, the Display Report stacks the results according
421 to the Focal Document element. For example, if Reference A has two relationship pairings to a
422 given Focal Document element and Reference B has two relationship pairings to the same Focal

Document element, the two Reference A relationships will be displayed in rows 1 and 2, followed by Reference B's relationships in rows 3 and 4, with the Focal Document element identifier in the leftmost column of all four rows.

Hover-over 'Tool Tips' are provided with descriptions when the User scrolls the pointer over the column headers. Figure 6 shows an example of a tool tip when a User hovers above the "Reference Element Description" column header. Likewise, the Cybersecurity Framework Core definitions are displayed using the same Tool Tips behavior when a User hovers over the Framework Element identifier displayed in the leftmost column.

Table 2 provides a detailed description of the Display Report column headers.

Table 2: Display Report Column Header Descriptions

Field Name	Description
Framework Element	The identifier of the Focal Document element being mapped
Informative Reference Name	The name by which the Informative Reference listing will be referred
Reference Document Element	The identifier of the Reference Document element being mapped
Rationale	The processes, principles, or methods used to map the Reference Document element to the Focal Document element. This will be one of the following: • Syntactic—The two elements are character-by-character identical. • Semantic—The two elements are saying the same thing, although they may say it in different ways. • Functional—The two elements cause the same result, although they may accomplish that result in different ways.
Relationship	The type of logical relationship the Reference Document element asserts compared to the Focal Document element. The SME conducting the mapping should focus on the perceived intent of the statement. This will be one of the following: • Subset of—The Focal Document element is a subset of the Reference Document element. In other words, the Reference Document element contains everything the Focal Document element does, plus more. • Intersects with—The two elements have some overlap, but each includes things the other does not. • Equal to—The two elements are very similar (not necessarily identical). • Superset of—The Focal Document element is a superset of the Reference Document element. In other words, the Focal Document element contains everything the Reference Document element does, plus more. • Not related to—The two elements do not have anything in common.
Reference Element Description	The description of the Reference Document element
Comments	Additional information useful to NIST or an implementer of the Informative Reference
Group	The designation given to a Reference Document element when it is part of a group of Reference Document elements that correlates to a Focal Document element

3.5 Report Downloads

After creating a Display Report, multiple report download options are available, as depicted in the upper right corner of Figure 7: links to "Download the CSV File" (comma-separated values) and "Download the JSON File" (JavaScript Object Notation).[2] Clicking on a link causes the corresponding report file format to be downloaded.

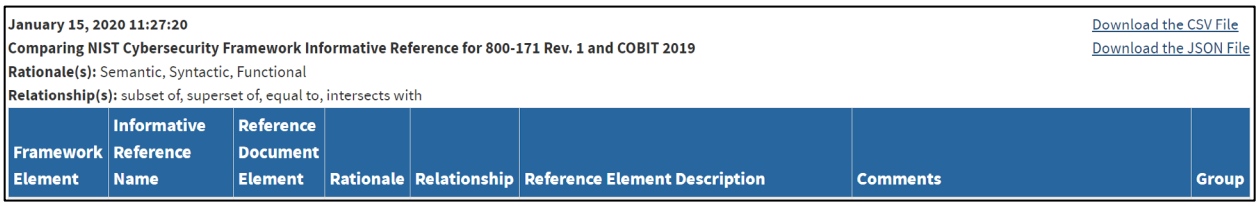
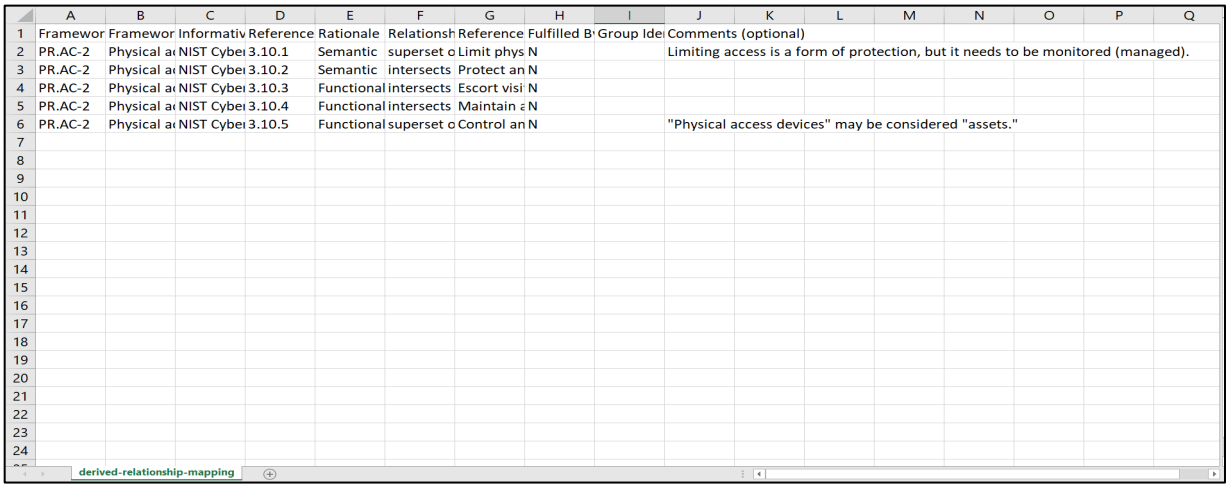


Figure 7: Report Download Options

The report downloads contain more information than the Display Report (for example, the Cybersecurity Framework Element description) for more convenient human comparison and automated processing.[3]

3.5.1 Report Download in CSV Format

The CSV format is a common format that is easily ingested into a spreadsheet program where searching and sorting functions can be performed. Those functions are not available via the DRM Analysis Tool. Figure 8 represents a sample CSV report. The CSV file is consistent with the columns of the OLIR Informative Reference template used by Reference Developers in NISTIR 8204 [2].



	A	B	C	D	E	F	G	H	I	J
1	Framewor	Framewor	Informativ	Reference	Rationale	Relationsh	Reference	Fulfilled B	Group Ide	Comments (optional)
2	PR.AC-2	Physical a	NIST Cybe	3.10.1	Semantic	superset o	Limit phys	N		Limiting access is a form of protection, but it needs to be monitored (managed).
3	PR.AC-2	Physical a	NIST Cybe	3.10.2	Semantic	intersects	Protect an	N		
4	PR.AC-2	Physical a	NIST Cybe	3.10.3	Functional	intersects	Escort visi	N		
5	PR.AC-2	Physical a	NIST Cybe	3.10.4	Functional	intersects	Maintain a	N		
6	PR.AC-2	Physical a	NIST Cybe	3.10.5	Functional	superset o	Control an	N		"Physical access devices" may be considered "assets."

Figure 8: Sample CSV Report

[2] The CSV and JSON download links only become available after the Display Report is generated.
[3] See NISTIR 8204 [2] for additional field descriptions.

3.5.2 Report Download in JSON Format

The JSON format provides the report data in a format that many tools can utilize to perform more in-depth analyses not available from the DRM Analysis Tool. The JSON file depicted in Figure 9 shows how the data is displayed. The JSON's file contents are consistent with the columns of the OLIR Informative Reference template used by Reference Developers in NISTIR 8204 [2].


```
{
  "Report_Date": "2020-01-10T13:53:15.148448-05:00",
  "Information_Reference_Name_1": "",
  "Information_Reference_Name_2": "",
  "Function": [
    "PR"
  ],
  "Category": [
    "PR.AC"
  ],
  "Subcategory": [
    "PR.AC-2"
  ],
  "Rationale": [
    "Semantic",
    "Syntactic",
    "Functional"
  ],
  "Relationship": [
    "subset of",
    "superset of",
    "equal to",
    "intersects with"
  ],
  "Derived_Relationships": [
    {
      "Framework_Element": "PR.AC-2",
      "Framework_Element_Description": "Physical access to assets is managed and protected",
      "Informative_Reference_Name": "NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1",
      "Reference_Document_Element": "3.10.1",
      "Relationship": "superset of",
      "Rationale": "Semantic",
      "Reference_Document_Element_Description": "Limit physical access to organizational systems, equipment, an
      "Comments": "Limiting access is a form of protection, but it needs to be monitored (managed).",
      "Fulfilled_By": "N",
      "Group_Identifier": ""
    },
```


Figure 9: Sample JSON Report

3.6 Common Use Cases

The DRM Analysis Tool output displays authoritative relationships. When a User compares the relationships from different Reference Documents and infers additional relationships among them, those inferred—*derived*—relationships are non-authoritative, but they are still useful for a variety of use cases, one group of which is discussed in the following subsection. Additional use cases will be added to a subsequent version of this document.

3.6.1 Comparative Analysis of Cybersecurity Documents and Controls

People often need to compare two cybersecurity documents for a variety of reasons, to include demonstrating where the documents' cybersecurity controls are similar and where gaps exist. This is true for cybersecurity document authors, cybersecurity auditors, and cybersecurity control implementers alike.

3.6.1.1 Without OLIR DRM

Before the OLIR Program, a person analyzing documents was often forced to conduct a manual comparison, typically by copying the contents of both documents into a spreadsheet for easier searching and sorting. The analyst would then resort to using section headers as a starting point for the comparison because of a lack of consistent identifiers within the documents. For example, if an analyst was comparing the CIS Controls with NIST SP 800-171, the analyst would start within the CIS Reference Document at "CIS Control 1: Inventory and Control Hardware Assets", then proceed to SP 800-171 and find a section where a similar element to the CIS element might be documented. For this specific example, the analyst might select the "Access Control" section 3.1 of SP 800-171 and read through each of its basic and derived security requirements to identify relationships.

To save time, an analyst might try to leverage existing document mappings from SMEs. In this specific example, the analyst could leverage the mappings within SP 800-171 to SP 800-53 controls, and also leverage the NIST Cybersecurity Framework, which contains mappings from its elements to both SP 800-53 controls and the CIS Controls. So the NIST Cybersecurity Framework could serve as a transitive link for identifying commonality between the CIS Controls and SP 800-171. SP 800-171 Requirement 3.1.16 lists a relationship with SP 800-53 control AC-18. After searching the Cybersecurity Framework Core for mappings to AC-18, it is determined that there is a relationship listed with CIS controls 8, 12, and 15. The analyst could then focus their comparative analysis on these three controls.

This process would be repeated for both the sub-controls of CIS and the basic and derived requirements of SP 800-171. Multiply this process by hundreds of analysts performing the same brute force process, and two problems quickly emerge: 1) the different opinions of analysts result in inconsistent associations, and 2) the analysts duplicate an enormous amount of effort. Streamlining this process is the main reason the OLIR DRM capability was created.

3.6.1.2 With OLIR DRM

Since OLIR Catalog entries must comply with NISTIR 8204, OLIR submissions are already decomposed and associated with a Focal Document (in this case, the NIST Cybersecurity Framework) using standard identifiers created by the document submitters. The stacked Display Report and report download options provide Users a convenient way to quickly view how one document may relate to another by leveraging the Focal Document. The DRM Analysis Tool automates the brute force comparison method for comparing Reference Documents, rendering transitive relationship possibilities for the analyst to consider. Even though the stacked reference comparison is not authoritative, since it is derived from inferences from authoritative first-order

SME statements, it represents a good starting point for various types of comparative analysis and research.

With much of the relationship data defined by the SME (OLIR Developer) already, a User can simply generate a full report between two Reference Documents, selecting all desired Rationale and Relationship types, then exporting the stacked data output as CSV format for import into a spreadsheet application for searching and sorting. Using the example from Section 3.6.1.1, once the CSV file is imported, a User can sort the data by each Function, Category, and Subcategory to determine which SP 800-171 and CIS controls are listed. Then, using the Rationale and Relationship designations, the User can better understand the similarities and differences between the elements, and determine which relationships are relevant for their purposes.

To narrow down the potential for identifying strong associations between Reference Documents, a User could generate a Display Report using the Rationale and Relationship selectors to indicate association strength. By selecting options such as "Semantic" and "equal to," a User can parse the Display report for Reference relationships that have a better chance of relevance than, for example, what the options of "Functional" and "intersection" might provide.

Another popular use case is conducting a gap analysis between documents. For example, if an analyst knows their organization already implements the CIS Controls and NIST publishes a new version of SP 800-171, the analyst can generate a Display Report selecting the "not-related to" Relationship option. This report may contain data that is not relatable to the NIST CSF, but it does not preclude the data from relating to other Reference Documents. For example, just because SP 800-171 and CIS have elements that do not map to the Cybersecurity Framework does not mean that the two Reference Documents are unrelated to each other.

In summary, the benefits to the User include quicker analysis, the ability to leverage expert assertions, more structure in the analysis process, and better insight into the logic of the OLIR Developer.

4 Additional Information for Informative Reference Developers

This section provides information for Informative Reference Developers that supplements the information in Section 3 on the OLIR Catalog.

4.1 Informative Reference Lifecycle

The Informative Reference lifecycle within the OLIR Program comprises the following steps for each individual Informative Reference:

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 to the specifications of NISTIR 8204.
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 NISTIR 8204 specifications, 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 lifecycle. 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).

4.2 OLIR Validation Tool

The OLIR Validation Tool (https://www.nist.gov/cyberframework/informative-references/validation-tool) is helpful for Developers who are creating or refining an Informative Reference submission. The Validation Tool ensures syntactic compliance with the specifications of the Informative Reference template and NISTIR 8204. The tool is a .jar file, and the link to the tool includes prerequisite information and various options available for Developers.

565 ## References

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

[2] Barrett MP, Keller N, Quinn SD, Smith MC (2019) Cybersecurity Framework Online Informative References (OLIR) Submissions: Specification for Completing the OLIR Template. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8204, Includes updates as of August 01, 2019. https://doi.org/10.6028/NIST.IR.8204

[3] Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. (The White House, Washington, DC), DCPD-201300091, February 12, 2013. https://www.govinfo.gov/app/details/DCPD-201300091

[4] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283

566

Appendix A—Acronyms

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

CIS	Center for Internet Security
CSRC	Computer Security Resource Center
CSV	Comma-Separated Values
DRM	Derived Relationship Mapping
EO	Executive Order
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
IR	Interagency or Internal Report
ITL	Information Technology Laboratory
JSON	JavaScript Object Notation
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
OLIR	Online Informative Reference
OMB	Office of Management and Budget
SME	Subject Matter Expert
SP	Special Publication
URL	Uniform Resource Locator
USG	United States Government

570 ## Appendix B—Glossary

Developer	A person, team, or organization that creates an Online Informative Reference.
Focal Document	A source document that is used as the basis for comparing a concept with a concept from another document. As of this writing, the OLIR Program has a single Focal Document: the Cybersecurity Framework.
Focal Document Element	A discrete section, sentence, phrase, or other identifiable piece of content of a Focal Document.
Informative Reference	A relationship between a Reference Document Element and a Focal Document Element.
Non-Owner	An Informative Reference produced by anyone who is NOT the owner of the Reference Document.
OLIR Catalog	The OLIR Program's online repository for hosting and sharing OLIRs.
Online Informative Reference (OLIR)	An Informative Reference expressed in NISTIR 8204-compliant format and stored in the OLIR Catalog.
Owner	An Informative Reference produced by the owner of the Reference Document.
Reference	See "Informative Reference".
Reference Document	A document being compared to a Focal Document. Examples include traditional documents, products, services, education materials, and training.
Reference Document Element	A discrete section, sentence, phrase, or other identifiable piece of content of a Reference Document.
User	A person, team, or organization that accesses or otherwise uses an Online Informative Reference.

571

Appendix C—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.

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 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