

1 **Draft (2nd) NISTIR 8278**

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

5 *Program Overview and OLIR Uses*

6  
7 Nicole Keller  
8 Stephen Quinn  
9 Karen Scarfone  
10 Matthew Smith  
11 Vincent Johnson  
12  
13  
14  
15  
16

17 This publication is available free of charge from:  
18 <https://doi.org/10.6028/NIST.IR.8278-draft2>  
19

22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51

Draft (2nd) NISTIR 8278

# National Cybersecurity Online Informative References (OLIR) Program:

*Program Overview and OLIR Uses*

Nicole Keller  
Stephen Quinn  
*Computer Security Division  
Information Technology Laboratory*

Matthew Smith  
*Huntington Ingalls Industries  
Annapolis Junction, MD*

Karen Scarfone  
*Scarfone Cybersecurity  
Clifton, VA*

Vincent Johnson  
*Electrosoft Services, Inc.  
Reston, VA*

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.IR.8278-draft2>

August 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*

52 National Institute of Standards and Technology Interagency or Internal Report 8278  
53 31 pages (August 2020)

54 This publication is available free of charge from:  
55 <https://doi.org/10.6028/NIST.IR.8278-draft2>

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

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

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

69 **Public comment period: August 4, 2020 through September 4, 2020**

70 National Institute of Standards and Technology  
71 Attn: Applied Cybersecurity Division, Information Technology Laboratory  
72 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000  
73 Email: [olir@nist.gov](mailto:olir@nist.gov)

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

75

76

## Reports on Computer Systems Technology

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

85

### Abstract

86 The National Cybersecurity Online Informative References (OLIR) Program is a NIST effort to  
87 facilitate subject matter experts in defining standardized Online Informative References (OLIRs),  
88 which are relationships between elements of their documents and elements of other documents  
89 like the NIST Cybersecurity Framework. The OLIR Program provides a standard format for  
90 expressing OLIRs as well as a centralized location for displaying them. This report describes the  
91 OLIR Program, focusing on explaining what OLIRs are, what benefits they provide, how anyone  
92 can search and access OLIRs, and how subject matter experts can contribute OLIRs.

93

### Keywords

94 catalog; Cybersecurity Framework; informative references; mapping; National Cybersecurity  
95 OLIR Program; Online Informative References (OLIRs).

96

97

## **Acknowledgments**

98 Thanks to all of those who contributed to or commented on this document.

99

100

## **Audience**

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

104

105

## **Trademark Information**

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

107

108

## **Note to Readers**

109 As of this writing, NIST plans on soon providing downloaded Javascript Object Notation (JSON)  
110 formats for the three focal document templates (Cybersecurity Framework version 1.1, the  
111 Privacy Framework version 1.0, and Special Publication 800-53 Rev. 4) and all current NIST-  
112 developed OLIRs within the OLIR Catalog.

113

114

## Call for Patent Claims

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

121

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

124

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

127

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

131

132 i. under reasonable terms and conditions that are demonstrably free of any unfair  
133 discrimination; or

134 ii. without compensation and under reasonable terms and conditions that are  
135 demonstrably free of any unfair discrimination.

136

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

142

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

145

146 Such statements should be addressed to: [olir@nist.gov](mailto:olir@nist.gov)

147

148 **Executive Summary**

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

158 The National Cybersecurity Online Informative References Program is a NIST effort to facilitate  
159 subject matter experts (SMEs) in defining standardized online informative references (OLIRs)  
160 between elements of their cybersecurity, privacy, and workforce documents and elements of  
161 other cybersecurity, privacy, and workforce documents like the Cybersecurity Framework. At  
162 this stage of the OLIR Program evolution, the initial focus is on relationships to cybersecurity  
163 and privacy documents.

164 The OLIRs are in a simple standard format defined by NIST Interagency or Internal Report (IR)  
165 8278A, *National Cybersecurity Online Informative References (OLIR) Program: Submission*  
166 *Guidance for OLIR Developers* (“NISTIR 8278A”) [2], and they are displayed in a centralized  
167 location. By following this approach, cybersecurity document owners can use the OLIR Program  
168 as a mechanism for communicating with owners and users of other cybersecurity documents.  
169 Given the OLIR Program’s decentralized nature, cybersecurity document owners also have the  
170 flexibility to update their documents and then update their OLIRs according to their own unique  
171 requirements and schedules.

172 The OLIR Program integrates ongoing NIST projects that respond to administrative and  
173 legislative requirements, including those for the Cybersecurity Framework under Executive  
174 Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, [3] released in February  
175 2013, and the Federal Information Security Modernization Act of 2014 [4], which amended the  
176 Federal Information Security Management Act of 2002 (FISMA). The OLIR Program also  
177 addresses many Office of Management and Budget (OMB) memoranda that address specific  
178 cybersecurity issues and comprise large sets of regulations with which organizations must  
179 comply. The OLIR Program can represent relationships to any authoritative documents,  
180 products, or services. These resources can be generated from national and international  
181 standards, guidelines, frameworks, and regulations to policies for individual organizations,  
182 sectors, or jurisdictions.

183 The purpose of this document is to describe the National Cybersecurity OLIR Program and  
184 explain the use, benefits, and management of the OLIR Catalog—the online location for sharing  
185 OLIRs—for both the SMEs contributing OLIRs to it and the Catalog’s users. The content of this  
186 document complements that of NISTIR 8278A [2], which provides additional information for the  
187 SMEs defining OLIRs and submitting them to the OLIR Program. SMEs should read this  
188 document first, then NISTIR 8278A.

189 **Table of Contents**

190 **Executive Summary ..... v**

191 **1 Introduction ..... 1**

192 1.1 Purpose and Scope ..... 1

193 1.2 Document Structure ..... 1

194 **2 Overview of the National Cybersecurity OLIR Program ..... 2**

195 **3 Common Uses of the OLIR Catalog..... 4**

196 3.1 Reference Data..... 4

197 3.1.1 Tier 1 – Informative References ..... 7

198 3.1.2 Tier 2 – Derived Relationship Mappings (DRMs) ..... 7

199 3.2 The OLIR Catalog ..... 8

200 3.3 The DRM Analysis Tool ..... 12

201 3.4 Display Report ..... 13

202 3.5 Report Downloads ..... 15

203 3.5.1 Report Download in CSV Format ..... 16

204 3.5.2 Report Download in JSON Format ..... 16

205 3.6 Common Use Cases..... 17

206 3.6.1 Comparative Analysis of Cybersecurity Documents and Controls..... 17

207 **References ..... 20**

208 **List of Appendices**

209

210 **Appendix A— Acronyms ..... 21**

211 **Appendix B— Glossary ..... 22**

212

213 **List of Figures**

214 Figure 1: Relationship Types..... 4

215 Figure 2: Relative Strength of Relationships ..... 6

216 Figure 3: Multiple Documents Related to a Focal Document ..... 8

217 Figure 4: OLIR Catalog Page ..... 9

218 Figure 5: Informative Reference More Details Page..... 10

219 Figure 6: DRM Analysis Tool Home Page ..... 12

220 Figure 7: Multi-Select Example ..... 13

221 Figure 8: Display Report Example..... 14

222 Figure 9: Report Download Options ..... 15  
223 Figure 10: Sample CSV Report..... 16  
224 Figure 11: Sample JSON Report..... 17  
225

226 **List of Tables**

227 Table 1: Relationship Type Descriptions ..... 5  
228 Table 2: Informative Reference More Details Description Fields..... 10  
229 Table 3: Display Report Column Header Descriptions ..... 15  
230

## 231 **1 Introduction**

### 232 **1.1 Purpose and Scope**

233 The purpose of this document is to describe the National Cybersecurity Online Informative  
234 References (OLIR) Program and explain the use and benefits of the OLIR Catalog for  
235 Informative Reference Developers (“Developers”) and Informative Reference Users (“Users”) of  
236 the OLIR Program.

237 In addition to this document, Developers may also be interested in NIST Interagency or Internal  
238 Report (IR) 8278A, *National Cybersecurity Online Informative References (OLIR) Program:  
239 Submission Guidance for OLIR Developers* (“NISTIR 8278A”) [2]. NISTIR 8278A is intended  
240 to assist Developers as they complete the spreadsheet template for submitting their OLIRs to the  
241 Program. Developers should read this document first, then NISTIR 8278A.

### 242 **1.2 Document Structure**

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

- 244 • Section 2 provides an overview of the OLIR Program.
- 245 • Section 3 describes common uses of the OLIR Catalog relevant to both Developers and  
246 Users.
- 247 • The References section lists the references for the publication.
- 248 • Appendix A contains acronyms used throughout the document.
- 249 • Appendix B provides a glossary of terminology used throughout the document.

250

## 251 **2 Overview of the National Cybersecurity OLIR Program**

252 In a general sense, an informative reference, sometimes called a mapping, indicates how one  
253 document relates to another document. Informative references were originally documented  
254 within the original version of the NIST Cybersecurity Framework document. While the concept  
255 of informative references was well received, the static nature of the Cybersecurity Framework  
256 document meant that some of its informative references became outdated as the documents they  
257 referenced were updated.

258 Within the context of the National Cybersecurity OLIR Program, an *Informative Reference*  
259 (abbreviated as *Reference*) indicates the relationship(s) between elements of two documents. The  
260 source document, called the *Focal Document*, is used as the basis for the document comparison.  
261 The second document is called the *Reference Document*. Note that a Focal Document or a  
262 Reference Document is not necessarily in a traditional document format—either could be a  
263 product, service, training, etc. A *Focal Document element* or a *Reference Document element* is a  
264 discrete section, sentence, phrase, or other identifiable piece of content of a document.

265 As of this writing, the OLIR Program has three Focal Documents: the *Framework for Improving*  
266 *Critical Infrastructure Cybersecurity* (“Cybersecurity Framework”) version 1.1 [1], the *Privacy*  
267 *Framework: A Tool for Improving Privacy through Enterprise Risk Management* (“Privacy  
268 Framework”) version 1.0 [5], and Special Publication 800-53 Revision 4, *Security and Privacy*  
269 *Controls for Federal Information Systems and Organizations* (“SP 800-53 Rev. 4”) [6].

270 Although using Informative References can significantly improve understanding of documents  
271 within organizations, using an Informative Reference does not demonstrate or certify that an  
272 organization complies with a document.

273 The OLIR Program provides an online site—the OLIR Catalog—for displaying, sharing, and  
274 comparing Informative References. The OLIR Program defines a simple format in NISTIR  
275 8278A [2] for expressing References in the OLIR Catalog in a standardized, consistent manner.  
276 The OLIR Program offers several benefits, including the following:

- 277 • There are many potential Reference Documents, so the OLIR Program provides a single,  
278 easy-to-use place where people can obtain information on many Reference Documents  
279 and analyze their relationships. This approach also significantly reduces the time that  
280 organizations need to research and analyze their current and target cybersecurity  
281 activities and to communicate with others regarding those activities. Without a central  
282 location, finding and comparing cybersecurity resources can be difficult.
- 283 • The OLIR Program increases transparency, alignment, and harmonization of definitions  
284 and concepts across Reference Documents.
- 285 • Standardizing how References are expressed makes them more consistent, clear, usable,  
286 repeatable, and organizable, and it provides a way for automation technologies to ingest  
287 and utilize them.

- 288 • Having a centralized OLIR Program allows for the authentication of each Reference's  
289 source and identifies whether or not the Reference was provided by a verified SME on  
290 the Reference Document.
- 291 • The OLIR Program employs additional mathematic rigor (e.g., standard set theory  
292 principles, such as subset, superset, equal, intersect, and discrete logic) to express  
293 References instead of just relying on prose, which is ambiguous and subject to individual  
294 interpretation.
- 295 • The OLIR Program increases the integration of NIST guidance, which is produced in  
296 support of United States Government (USG) legislative and administrative  
297 responsibilities.

298 The OLIR Program also defines a formal process for vendors and other OLIR Developers to  
299 submit OLIRs to NIST [2]. This process includes guidance for creating high-quality, more  
300 usable, better documented OLIRs. It also defines a managed process for the review, update, and  
301 maintenance of OLIRs as Focal and Reference Documents are updated and revised.

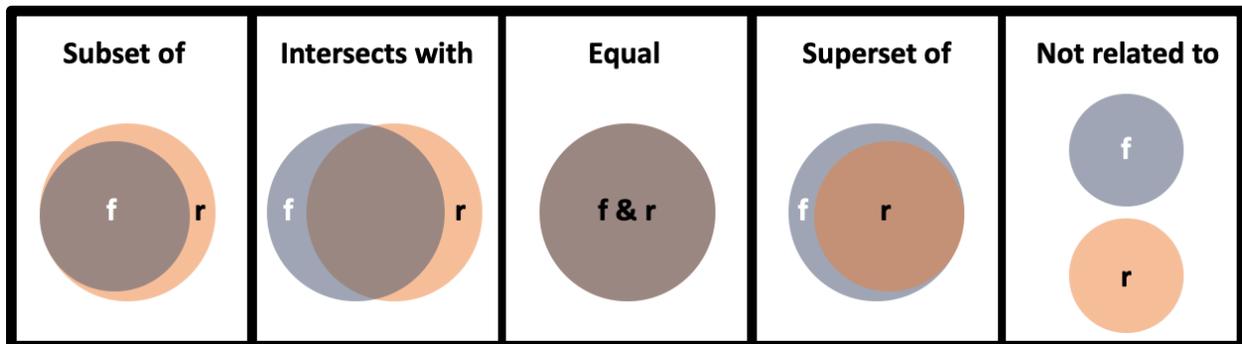
302 **3 Common Uses of the OLIR Catalog**

303 This section provides information on the use of the OLIR Catalog for both OLIR Developers and  
 304 Users. Section 3.1 explains the types of information that the Catalog contains. Section 3.2  
 305 reviews the interfaces for viewing and searching the OLIRs in the Catalog, as well as the  
 306 supporting information that the Catalog holds for each OLIR. Section 3.3 provides information  
 307 on an analysis tool that helps characterize relationships among Reference Documents. Section  
 308 3.4 explains how to generate comparative analysis reports between OLIRs at different levels of  
 309 abstraction, and Section 3.5 discusses how to download those reports. Finally, Section 3.6  
 310 introduces use cases for the OLIR Catalog.

311 **3.1 Reference Data**

312 The OLIR Catalog contains two types of information on the relationships between Focal  
 313 Documents and Reference Documents: Informative References and Derived Relationship  
 314 Mappings. These relationships are organized as *Reference Data* via the OLIR Catalog according  
 315 to the vetting processes delineated in NISTIR 8278A [2] with the objective of providing  
 316 transparency from the Informative Reference Developers for reproducibility and discussion by  
 317 Users.

318 Each relationship between a Reference Document element and a Focal Document element has a  
 319 *type*. The type indicates how the meanings of the two elements are related, and for each  
 320 relationship, the type will be one of the following, as depicted in Figure 1 (where “f” is a Focal  
 321 Document element and “r” is a Reference Document element) and further explained in Table 1.

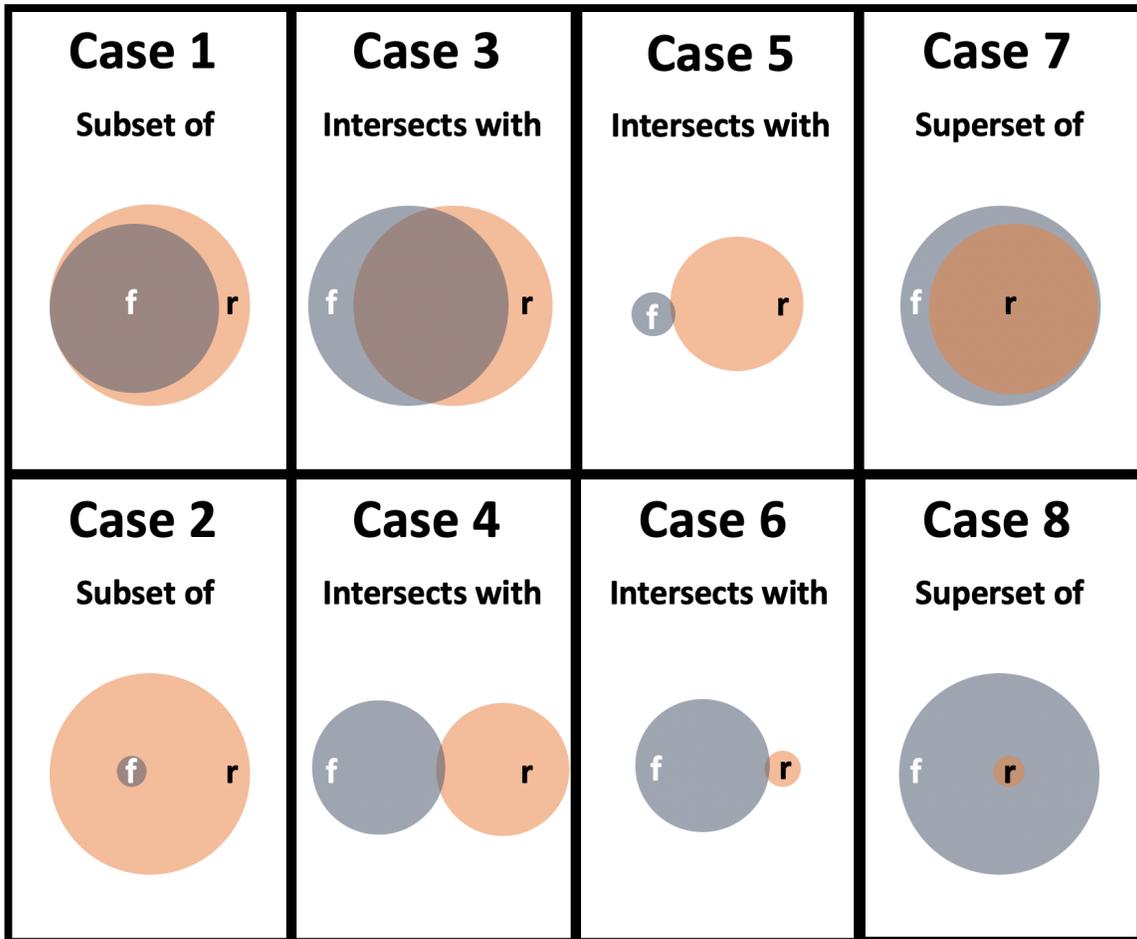


322  
323

Figure 1: Relationship Types



352 Another goal of the OLIR Program is to find ways to quantify the strength of a relationship,  
 353 which would help enable evaluating a relationship between two elements of different sizes.  
 354 Figure 2 illustrates how a single relationship type can encompass relationships of different  
 355 strengths. Case 1 shows a Focal Document element and a Reference Document element in a  
 356 Subset relationship with many common elements, while Case 2 shows a Subset relationship  
 357 where the two elements have fewer common elements. The OLIR Program encourages subject  
 358 matter experts making assertions to include a measure of the strength of comparable  
 359 relationships but does not prescribe a particular methodology for doing so.



360

361

**Figure 2: Relative Strength of Relationships**

362 Quantifying the strength of a relationship for an Informative Reference is optional, and its  
 363 omission should not be interpreted as negative. It is intended for lateral comparisons only, like  
 364 the Cybersecurity Framework and the Privacy Framework, and not comparisons of documents at  
 365 different levels, such as the Cybersecurity Framework and a research paper on a topic in  
 366 quantum cryptography. Non-lateral relationships are to be designated with “N/A.”

### 367 3.1.1 Tier 1 – Informative References

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

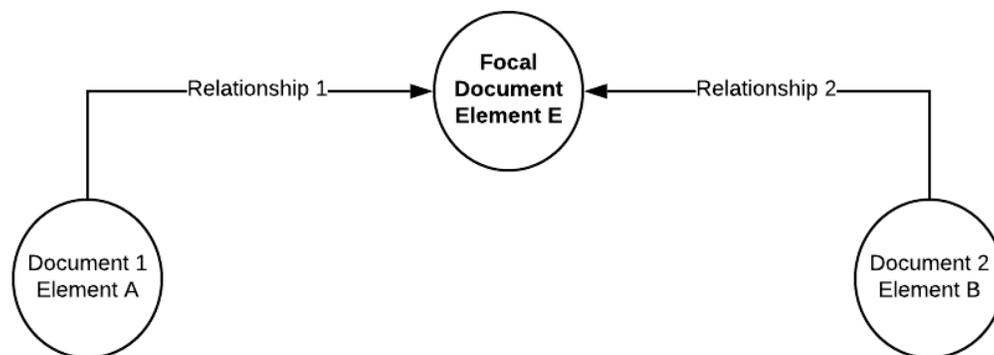
- 371 • **Owner:** These are produced by the owner of the Reference Document. For example,  
372 NIST is the owner of NIST SP 800-171 [7] and produced the Informative Reference for  
373 SP 800-171; therefore, the designation of “owner” is granted to the SP 800-171  
374 Informative Reference developed by NIST.
- 375 • **Non-Owner:** These are produced by anyone who is NOT the Reference Document  
376 owner. For example, if Organization A developed an Informative Reference for SP 800-  
377 171, the Informative Reference would be designated “non-owner.”

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

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

### 389 3.1.2 Tier 2 – Derived Relationship Mappings (DRMs)

390 Tier 2 Reference Data are the Derived Relationship Mappings (DRMs). DRMs are the result of  
391 using the relationships between Reference Documents and a Focal Document to make inferences  
392 about document-to-document relationships. Figure 3 depicts how a User could find a relationship  
393 between Reference Document 1 Element A and Reference Document 2 Element B based on their  
394 individual relationships to Focal Document Element E. DRMs are dynamically generated when a  
395 User utilizes the DRM Analysis Tool to search the OLIR Catalog on the OLIR website, as  
396 described in Section 3.3. The results of the search are displayed to the User, as shown in Figure  
397 8. DRMs serve as the foundation for gap and comparative analysis.



398

399

**Figure 3: Multiple Documents Related to a Focal Document**

400 The function of DRMs is to display relationships between Reference Documents and Focal  
 401 Documents. While the inferences that a User makes while using DRMs are informative, they are  
 402 not considered verified nor authoritative. DRMs help users of cybersecurity documents make  
 403 informed decisions regarding cybersecurity risk management activities.

404 These relationships, which are defined in NISTIR 8278A [2], do not indicate the relationships  
 405 among the Reference Documents. Therefore, in reference to Figure 3, if an organization  
 406 implements Document 1 Element A, that does not necessarily mean it is also implementing  
 407 Document 2 Element B. The two elements are potentially related. Even when the relationship is  
 408 “equal,” that does not mean the two elements are identical and does not imply that implementing  
 409 one element means compliance with the other element.

410 Another caveat about DRMs is that the elements being compared are often at different levels of  
 411 detail (sometimes referred to as “different levels of abstraction.”) For example, suppose someone  
 412 wants to compare Focal Document Element PR.AC-1, “Identities and credentials are issued,  
 413 managed, verified, revoked, and audited for authorized devices, users, and processes” [1], to  
 414 Reference Document Element IA-7, “Cryptographic Module Authentication,” which is defined  
 415 as “The information system implements mechanisms for authentication to a cryptographic  
 416 module that meet the requirements of applicable federal laws, Executive Orders, directives,  
 417 policies, regulations, standards, and guidance for such authentication” [6]. The Focal Document  
 418 Element is at a higher level than the Reference Document Element, which specifies, in detail,  
 419 one part of what the Focal Document Element encompasses. For some DRMs, the difference in  
 420 the level of detail of the elements being compared may be vast.

421 See Section 3.6 for common use cases for DRMs.

### 422 3.2 The OLIR Catalog

423 The OLIR Catalog<sup>1</sup> contains all of the Reference Data—Informative Reference data and  
 424 DRMs—for the National Cybersecurity OLIR Program. All Reference Data in the OLIR Catalog  
 425 has been validated against the requirements of NISTIR 8278A [2] and is displayed by default

<sup>1</sup> See <https://csrc.nist.gov/projects/cybersecurity-framework/informative-reference-catalog>.

426 according to the most recent OLIR received. The OLIR Catalog provides an interface for  
427 Developers and Users to view Informative References and analyze Reference Data.

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

432 Figure 4 shows the OLIR Catalog Page. From this page, Users can browse and search  
433 Informative Reference content in multiple ways. Users can search the entire OLIR catalog to  
434 locate and retrieve an Informative Reference using a variety of fields, such as Informative  
435 Reference (name), Reference Document, Posted Date, and Submitting Organization. Utilizing  
436 the dropdowns in the *Advanced Search* section, Users can search Informative References based  
437 on a focal document of their choice. Users can also locate and retrieve an Informative Reference  
438 using a variety of fields, such as the type of Authority or Category of Submitter that an  
439 Informative Reference is cataloged as. Additionally, Users can perform keyword searches of  
440 catalog content and sort the catalog columns within the table in a variety of different ways.

The screenshot shows the 'ADVANCED SEARCH' section of the OLIR Catalog Page. It includes several search filters: 'Focal Document' (set to 'Cybersecurity Framework v1.1'), 'Informative Reference Name', 'Reference Document', 'Posted Date' (with date pickers), 'Authority' (checkboxes for Non-Owner and Owner), 'Category of Submitter' (checkboxes for Academia, Other, Private Sector, and Public Sector), 'Keyword(s)', and 'Sort By' (set to 'Reference Document (A-Z)'). There are 'Search' and 'Reset' buttons at the bottom right of the search section.

Informative Reference (ver)	Reference Document	Posted Date	Focal Document	Submitting Organization	Authority	Category of Submitter
<a href="#">NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1 (1.0.0) (More Details)</a>	<a href="#">NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management</a>	05/19/20	Cybersecurity Framework v1.1	NIST	Owner	Public Sector

441

442

**Figure 4: OLIR Catalog Page**

443 Selecting the “More Details” link of an Informative Reference in the Catalog will display a  
444 description page, shown in Figure 5, that includes the General Information of an Informative  
445 Reference as provided by the Developer.

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

Cybersecurity Framework

**Download Informative Reference Resource**

<https://www.nist.gov/document/csf-sp800-171mappingxlsx>

**Informative Reference Information**

**Status:**  
Final

**Informative Reference Version:**  
1.0.0

**Focal Document 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](mailto:sec-cert@nist.gov)

**Category of Submitter:**  
Public Sector

**Dependencies/Requirements:**  
Stand-alone

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

[Generate Relationship Report](#)

---

SHA3-256

cbe5baedf9b40b6c14ddf90ee5877ba82c46b29810856f9eb196a3c3261bb7a6

---

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 06/07/2018

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

**Reference Developer:**  
NIST

**Posted Date:**  
November 13, 2019

446

447

**Figure 5: Informative Reference More Details Page**

448

Table 2 lists fields and descriptions of the information depicted on the More Details page in Figure 5.

449

450

**Table 2: Informative Reference More Details Description Fields**

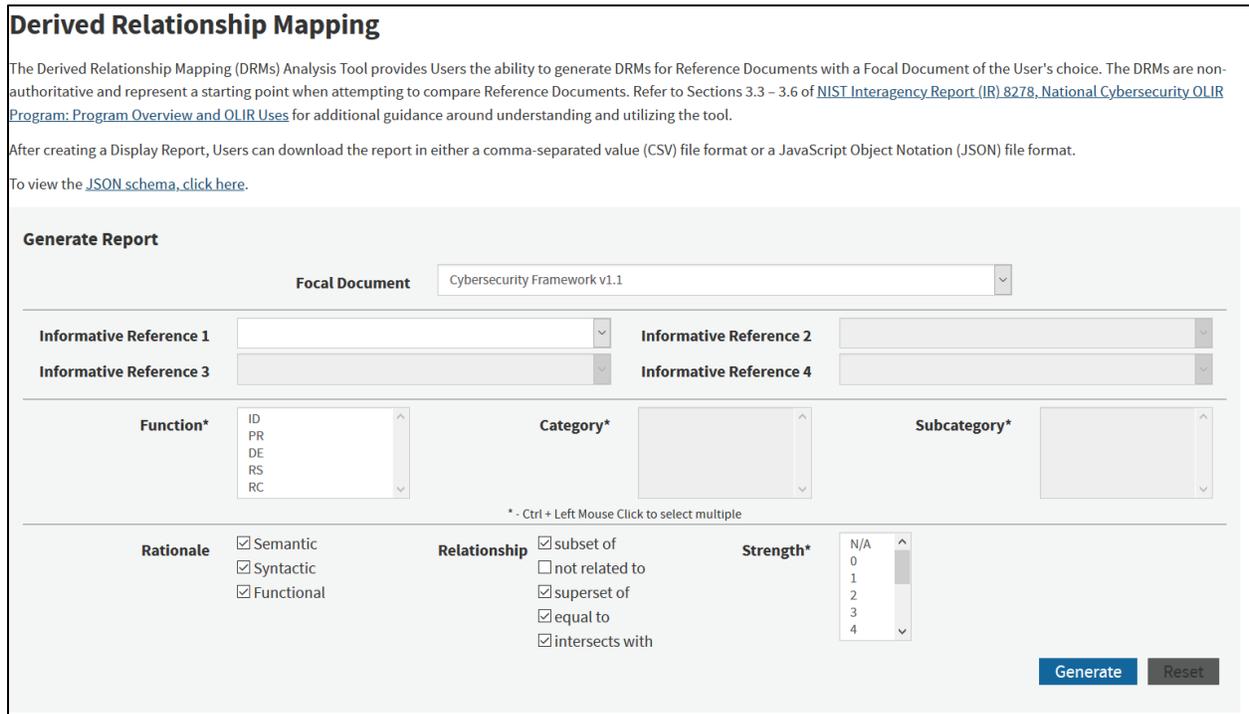
Field Name	Description
Informative Reference Name	The name by which the Informative Reference listing will be known. The format is a human-readable string of characters.
Focal Document	A source document that is used as the basis for comparing a concept with a concept from another document. As of this writing, the OLIR Program has three Focal Documents: the Cybersecurity Framework, the Privacy Framework, and SP 800-53 Rev. 4.
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)

Field Name	Description
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.
Focal Document Version	The Focal Document version used in creating the Informative Reference. NIST recommends that Developers begin with the latest Focal Document version. <sup>2</sup>
Summary	The purpose of the Informative Reference
Target Audience	The intended audience for the Informative Reference
Comprehensive	Whether the Informative Reference maps <i>all</i> 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
Category of Submitter	<p>The category type of the Informative Reference:</p> <ul style="list-style-type: none"> <li>• Public Sector: a governmental or regulatory agency, bureau, or board of the United States (Federal, state, local)</li> <li>• Private Sector: any incorporated group that provides products, services, or information and the products, services, or information covers topics related to the Focal Document</li> <li>• Academia: informative references which originate from educational institutions. Examples include universities, colleges, and research laboratories.</li> <li>• Other: informative references which do not fall into the previous categories are assigned the designation of “other.” Examples include standards development organizations and international governments.</li> </ul>
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 Informative Reference. The value is monitored to maintain data integrity of the 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 that the Reference Document was published and, if applicable, amended
Reference Document URL	The URL where the Reference Document can be viewed, downloaded, or purchased
Reference Developer	The organization(s) that created the Informative Reference
Posted Date	The date that a validated Informative Reference submission was added to the catalog for the draft public comment period or the final posting following the completion of the public comment period and adjudication process

<sup>2</sup> This field will be modified as additional Focal Documents are added to the OLIR Program.

451 **3.3 The DRM Analysis Tool**

452 The DRM Analysis Tool<sup>3</sup> provides Users with the ability to generate DRMs for Reference  
453 Documents with a Focal Document of the User’s choice. The DRMs are non-authoritative and  
454 represent a starting point when attempting to compare Reference Documents. Figure 6 depicts  
455 the homepage of the DRM Analysis Tool.



456  
457 **Figure 6: DRM Analysis Tool Home Page**

458 As Figure 6 shows, when accessing the DRM Analysis tool, Users must first select the Focal  
459 Document for comparative analysis. Users have the ability to display potential relationships of  
460 up to four Informative References at a time for a given Focal Document. Users can generate  
461 reports at any level (i.e., Function, Category, Subcategory) of the Cybersecurity Framework or  
462 Control Family, Security/Privacy Control, or Security Control Enhancements for the SP 800-53  
463 Rev. 4 Focal Document. When a User accesses this page, all rationale and relationships pairings  
464 (except for the “not related to” relationship) are pre-selected by default. To filter out any  
465 rationale or relationship selections, the User can deselect a checkbox as appropriate before  
466 generating a report.

467 By default, the Strength of Relationship field is left unselected. Users can generate reports with  
468 this field unselected to display every type of strength defined within the Informative Reference

<sup>3</sup> See <https://csrc.nist.gov/projects/cybersecurity-framework/derived-relationship-mapping>.

469 of their search criteria. Users can narrow their criteria by selecting a singular or multiple strength  
470 pairing for further analysis.

471 In addition to performing an analysis at an individual level (i.e., selecting one Function,  
472 Category, or Subcategory), Users also have the ability to display Informative References at  
473 multiple levels (i.e., selecting multiple Functions, Categories, and Subcategories or multiple  
474 Control Families, Security/Privacy Controls, or Security Control Enhancements). Figure 7  
475 displays an example of multiple Categories and Subcategories selected for User analysis when a  
476 User has selected the Cybersecurity Framework Focal Document. In this example, the two  
477 Categories being displayed are ID.AM and ID.BE along with Subcategories ID.AM-6 and  
478 ID.BE-1. The Strength of Relationship field has been left unselected.

479 To achieve this desired output, a User should first select the “Cybersecurity Framework v1.1”  
480 Focal Document from the drop-down menu. The User should then choose the Informative  
481 References for comparative analysis. Next, the User should select the ‘ID’ Function, which will  
482 result in the applicable Categories being displayed in the Category box. To select multiple  
483 Categories on a Windows computer, the user can hold the “Ctrl” key and click on the ID.AM and  
484 ID.BE Categories. On a macOS computer, the user can hold the “Command” key instead of the  
485 “Control” key. Choosing both ID.AM and ID.BE will cause all of the Subcategories within  
486 ID.AM and ID.BE to be displayed in the Subcategory box. Users can continue this selection  
487 behavior to select multiple Subcategories.

The screenshot shows a web interface titled "Generate Report". At the top, there is a "Focal Document" dropdown menu set to "Cybersecurity Framework v1.1". Below this are four "Informative Reference" dropdown menus. The first is set to "NIST Cybersecurity Framework Informative Reference for 800" and the second to "NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1". The other two are empty. Below the references are three multi-select dropdown menus: "Function\*" with "ID" selected, "Category\*" with "ID.AM" and "ID.BE" selected, and "Subcategory\*" with "ID.AM-6" and "ID.BE-1" selected. A note below these menus reads "\* - Ctrl + Left Mouse Click to select multiple". At the bottom, there are three sections: "Rationale" with checkboxes for "Semantic", "Syntactic", and "Functional" (all checked); "Relationship" with checkboxes for "subset of", "not related to", "superset of", "equal to", and "intersects with" (all checked); and "Strength\*" with a dropdown menu showing "N/A", "0", "1", "2", "3", and "4". At the bottom right are "Generate" and "Reset" buttons.

488

489

Figure 7: Multi-Select Example

### 490 3.4 Display Report

491 After selecting the ‘Generate’ option (see Figure 7), Users are presented with an on-screen  
492 output table. Figure 8 shows the results of comparing two Informative References at the  
493 individual PR.AC-2 Subcategory level with the Cybersecurity Framework Focal Document  
494 selected. This on-screen output is the *Display Report*.

**Report**

Jun 8, 2020 12:09:57

Focal Document: Cybersecurity Framework v1.1

Comparing NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1 and NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1

Function(s): PR Category(s): PR.AC Subcategory(s): PR.AC-2

Rationale(s): Semantic, Syntactic, Functional

Relationships(s): subset of, superset of, equal to, intersects with

**GENERATE DOWNLOADABLE REPORTS**

---

Generate a CSV Report File

Generate a JSON Report File

[OLIR JSON 1.2 Schema](#)

Focal Document Element	Informative Reference Name	Reference Document Element	Rationale	Relationship	Reference Element Description	Comments	Group	Strength
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).		N/A
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.			N/A
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.			N/A
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.			N/A
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."		N/A
PR.AC-2	NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1	PR.AC-P2	Functional	superset of	Physical access to data and devices is managed.			N/A

495

496

**Figure 8: Display Report Example**

497 **Understanding Section 3.1.2 of this document is a prerequisite to understanding the**  
 498 **Display Report.** Due to screen space limitations, the Display Report stacks the results according  
 499 to the Focal Document element. For example, if Reference A has two relationship pairings to a  
 500 given Focal Document element, and Reference B has two relationship pairings to the same Focal  
 501 Document element, the two Reference A relationships will be displayed in rows 1 and 2,  
 502 followed by Reference B’s relationships in rows 3 and 4, with the Focal Document element  
 503 identifier in the leftmost column of all four rows.

504 Hover-over ‘Tool Tips’ are provided with descriptions when the User scrolls the pointer over the  
 505 column headers. Figure 8 shows an example of a Tool Tip when a User hovers above the  
 506 “Reference Element Description” column header. Likewise, the Cybersecurity Framework Core  
 507 definitions are displayed using the same Tool Tips behavior when a User hovers over the Focal  
 508 Document Element identifier displayed in the leftmost column.

509 Table 3 provides a detailed description of the Display Report column headers.

510

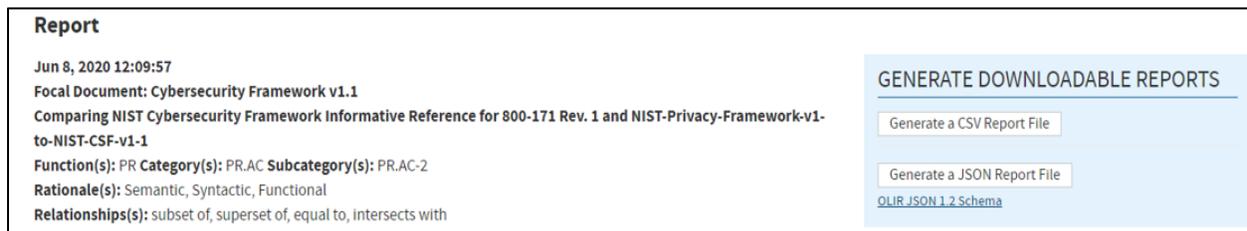
**Table 3: Display Report Column Header Descriptions**

Field Name	Description
Focal Document 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 explanation of why a Reference Document element and a Focal Document element are related. This will be one of the following: Syntactic, Semantic, or Functional.
Relationship	The type of logical relationship that the Reference Document Developer asserts compared to the Focal Document. The Developer conducting the assertion should focus on the perceived intent of each of the Reference and Focal Document elements. This will be one of the following, as depicted in Figure 1 (where “f” is a Focal Document element and “r” is a Reference Document element): Subset of, Intersects with, Equal to, Superset of, or Not related to.
Reference Element Description	The description of the Reference Document element
Comments	Notes to NIST or implementers
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
Strength of Relationship	The extent to which a Reference Document element and a Focal Document element are similar

511

512 **3.5 Report Downloads**

513 After creating a Display Report, multiple report download options are available, as depicted in  
 514 the right corner of Figure 9. Within “Generate Downloadable Reports” are links for a CSV  
 515 (comma-separated values) report file and a JSON (JavaScript Object Notation) report file.<sup>4</sup>  
 516 Clicking on a “Generate” link causes the corresponding report file format to be downloaded.



517

518

**Figure 9: Report Download Options**

<sup>4</sup> The CSV and JSON download links only become available after the Display Report is generated.

519 The report downloads contain more information than the Display Report (for example, Focal  
520 Document Element description) for more convenient human comparison and automated  
521 processing.<sup>5</sup>

522 **3.5.1 Report Download in CSV Format**

523 The CSV format is a common format that is easily ingested into a spreadsheet program where  
524 searching and sorting functions can be performed. Those functions are not available via the  
525 DRM Analysis Tool. Figure 10 represents a sample CSV report. The CSV file is consistent with  
526 the columns of the OLIR Informative Reference Focal Document template used by Reference  
527 Developers in NISTIR 8278A [2].

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Focal Document	Focal Document	Informative Reference	Rationale	Relationship Reference	Fulfilled By	Group Identifier	Comment	Strength of Relationship				
2	PR.AC-2	Physical access	NIST Cyber 3.10.1	Semantic	superset o	Limit phys N				Limiting at	N/A		
3	PR.AC-2	Physical access	NIST Cyber 3.10.2	Semantic	intersects	Protect an N					N/A		
4	PR.AC-2	Physical access	NIST Cyber 3.10.3	Functional	intersects	Escort visit N					N/A		
5	PR.AC-2	Physical access	NIST Cyber 3.10.4	Functional	intersects	Maintain z N					N/A		
6	PR.AC-2	Physical access	NIST Cyber 3.10.5	Functional	superset o	Control an N				"Physical z	N/A		
7	PR.AC-2	Physical access	NIST-Privacy PR.AC-P2	Functional	superset o	Physical at N					N/A		
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													
21													
22													
23													
24													
25													

528  
529 **Figure 10: Sample CSV Report**

530 **3.5.2 Report Download in JSON Format**

531 The JSON format provides the report data in a format that many tools can utilize to perform  
532 more in-depth analyses that are not available using the DRM Analysis Tool. The JSON file  
533 depicted in Figure 11 shows how the data is displayed. The JSON’s file contents are consistent  
534 with the columns of the OLIR Informative Reference Focal Document template used by  
535 Reference Developers in NISTIR 8278A [2].

<sup>5</sup> See NISTIR 8278A [2] for additional field descriptions.

```

{
  "Focal_Document": "Cybersecurity Framework v1.1",
  "Report_Date": "2020-06-08T12:22:53.6490936-04:00",
  "Information_Reference_Name_1": "NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1",
  "Information_Reference_Name_2": "NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1",
  "Function": [
    "PR"
  ],
  "Category": [
    "PR.AC"
  ],
  "Subcategory": [
    "PR.AC-2"
  ],
  "Rationale": [
    "Semantic",
    "Syntactic",
    "Functional"
  ],
  "Relationship": [
    "subset of",
    "superset of",
    "equal to",
    "intersects with"
  ],
  "Derived_Relationships": [
    {
      "Focal_Document_Element": "PR.AC-2",
      "Focal_Document_Element_Description": "Physical access to assets is managed and protected",
      "Security_Control_Baseline": "",
      "Informative_Reference_Name": "NIST Cybersecurity Framework Informative Reference for 800-171 Rev. 1",
      "Reference_Document_Element": "3.10.1",
      "Relationship": "superset of",
      "Strength_of_Relationship": "N/A",
      "Rationale": "Semantic",
      "Reference_Document_Element_Description": "Limit physical access to organizational systems, equipment, and the",
      "Comments": "Limiting access is a form of protection, but it needs to be monitored (managed).",
      "Fulfilled_By": "N",
      "Group_Identifier": ""
    }
  ],
}

```

536

537

Figure 11: Sample JSON Report

### 538 3.6 Common Use Cases

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

#### 544 3.6.1 Comparative Analysis of Cybersecurity Documents and Controls

545 Users often need to compare two cybersecurity or privacy documents for a variety of reasons,  
 546 such as demonstrating where the documents' cybersecurity controls are similar and where gaps  
 547 exist. This is true for cybersecurity or privacy document authors, auditors, and control  
 548 implementers alike.

**549 3.6.1.1 Without OLIR DRM**

550 Before the OLIR Program, a person analyzing documents was often forced to conduct a manual  
551 comparison, typically by copying the contents of both documents into a spreadsheet for easier  
552 searching and sorting. The analyst would then likely resort to using section headers as a starting  
553 point for the comparison because of a lack of consistent identifiers within the documents. For  
554 example, if an analyst were comparing the Cybersecurity Framework with NIST SP 800-171 [7],  
555 they would start within the Cybersecurity Framework Reference Document at the “Asset  
556 Management (ID.AM) Category,” then proceed to SP 800-171 and find a section where an  
557 element similar to the Cybersecurity Framework element might be documented. For this  
558 example, the analyst might select Section 3.4, “Configuration Management,” of SP 800-171 and  
559 read through each of its basic and derived security requirements to identify relationships.

560 To save time, an analyst might try to leverage existing document mappings from SMEs. In this  
561 example, the analyst could leverage the mappings within SP 800-171 to SP 800-53 [6] controls,  
562 as well as the NIST Cybersecurity Framework, which contains mappings from its elements to SP  
563 800-53 controls. So, SP 800-53 could serve as a transitive link for identifying commonality  
564 between the Cybersecurity Framework and SP 800-171. SP 800-171 Requirement 3.4.1 lists a  
565 relationship with SP 800-53 control CM-8. After searching the Cybersecurity Framework Core  
566 for mappings to CM-8, it is determined that there is a relationship listed for subcategories  
567 ID.AM-1, ID.AM-2, PR.DS-3, and DE.CM-7. The analyst could then focus their comparative  
568 analysis on these controls.

569 This process would be repeated for all of the categories and subcategories within the  
570 Cybersecurity Framework and the basic and derived requirements of SP 800-171. Multiply this  
571 process by hundreds of analysts performing the same brute force process, and two problems  
572 quickly emerge: 1) the different opinions of analysts result in inconsistent associations, and 2)  
573 the analysts duplicate an enormous amount of effort. Streamlining this process is the main reason  
574 that the OLIR DRM capability was created.

**575 3.6.1.2 With OLIR DRM**

576 Since OLIR Catalog entries must comply with NISTIR 8278A [2], OLIR submissions are  
577 already decomposed and associated with a Focal Document (in this case, the NIST Cybersecurity  
578 Framework) using standard identifiers created by the document submitters. The stacked Display  
579 Report and report download options provide Users with a convenient way to quickly view how  
580 one document may relate to another by leveraging the Focal Document. The DRM Analysis Tool  
581 automates the brute force comparison method for comparing Reference Documents, rendering  
582 transitive relationship possibilities for the analyst to consider. Even though the stacked reference  
583 comparison is not authoritative since it is derived from inferences from authoritative first-order  
584 SME statements, it represents a good starting point for various types of comparative analysis and  
585 research.

586 With much of the relationship data defined by the SME (OLIR Developer) already, a User can  
587 simply generate a full report between two Reference Documents—selecting all desired Rationale  
588 and Relationship types and then exporting the stacked data output in CSV format to import it into

589 a spreadsheet application for searching and sorting reference data. For example, once the CSV  
590 file is imported, a User can sort the reference data by Functions, Categories, and Subcategories  
591 or Control Families, Security/Privacy Controls, or Security Control Enhancements (depending on  
592 the Focal Document selected.) Then, using the Rationale and Relationship designations, the User  
593 can better understand the similarities and differences between the elements and determine which  
594 relationships are relevant for their purposes.

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

600 Another popular use case involves conducting a gap analysis between documents. Here are some  
601 examples:

- 602 • If an analyst knows that their organization already implements the NIST Privacy  
603 Framework, and NIST publishes a new version of SP 800-171, the analyst can generate a  
604 Display Report selecting the “Not related to” Relationship option. This report may  
605 contain data that is not relatable to the NIST Cybersecurity Framework, but it does not  
606 preclude the data from relating to other Reference Documents. Just because SP 800-171  
607 and the Privacy Framework have elements that do not map to the Cybersecurity  
608 Framework does not mean that the two Reference Documents are unrelated to each other.
- 609 • An analyst could generate Display Reports in order to identify significant changes  
610 between two versions of the same document. First, the analyst could report on the  
611 relationships between the Privacy Framework and the current version of SP 800-171.  
612 Next, the analyst could report on the relationships between the Privacy Framework and a  
613 new draft revision of SP 800-171. Finally, the analyst could use a tool to compare those  
614 two reports and identify their differences.
- 615 • An analyst could identify the gaps that would need to be addressed if their organization  
616 adopted a new security framework by generating a Display Report comparing the  
617 Reference Documents they already comply with to the Reference Document for the new  
618 security framework.

619 A final gap analysis example involves a vendor of cybersecurity products and services. Such a  
620 vendor could generate a Display Report that shows which requirements from Reference  
621 Documents their products and services help to address. This provides a starting point for an  
622 analyst, who will need to do additional analysis for each identified requirement to determine the  
623 strength of each relationship.

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

627

**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 (2020) National Cybersecurity Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8278A. <https://doi.org/10.6028/NIST.IR.8278A-draft>
- [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>
- [5] National Institute of Standards and Technology (2020) The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0 (National Institute of Standards and Technology, Gaithersburg, MD). <https://doi.org/10.6028/NIST.CSWP.01162020>
- [6] 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>
- [7] Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-171r2>

628

629 **Appendix A—Acronyms**

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

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	NIST Interagency or Internal Report
OLIR	Online Informative References
OMB	Office of Management and Budget
SME	Subject Matter Expert
SP	Special Publication
URL	Uniform Resource Locator
USG	United States Government

631

632 **Appendix B—Glossary**

Developer	See <i>Informative Reference Developer</i> .
Focal Document	A source document that is used as the basis for comparing an element with an element from another document. As of this writing, the OLIR Program has three Focal Documents: the Cybersecurity Framework version 1.1, the Privacy Framework version 1.0, and SP 800-53 Rev. 4.
Focal Document Element	Any number and combination of organizational concepts (e.g., Functions, Categories, Subcategories, Controls, Control Enhancements) of a Focal Document.
Informative Reference	A relationship between a Focal Document Element and a Reference Document Element.
Informative Reference Developer	A person, team, or organization that creates an Informative Reference and submits it to the OLIR Program.
Non-Owner	An Informative Reference produced by anyone who is NOT the owner of the Reference Document.
OLIR Catalog	The OLIR Program's online site for sharing OLIRs.
Online Informative Reference (OLIR)	An Informative Reference expressed in NISTIR 8278A-compliant format and shared by the OLIR Catalog.
Owner	An Informative Reference produced by the owner of the Reference Document.
Reference	See <i>Informative Reference</i> .
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.

633