

**NIST Internal Report
NIST IR 8278r1 ipd**

National Online Informative References (OLIR) Program:

Overview, Benefits, and Use

Initial Public Draft

Nicole Keller
Stephen Quinn
Karen Scarfone
Matthew C. Smith
Vincent Johnson

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8278r1.ipd>

**NIST Internal Report
NIST IR 8278r1 ipd**

**National Online Informative
References (OLIR) Program:
*Overview, Benefits, and Use***

Initial Public Draft

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

Matthew C. Smith
Huntington Ingalls Industries

Karen Scarfone
Scarfone Cybersecurity

Vincent Johnson
Electrosoft Services, Inc.

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8278r1.ipd>

December 2022



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

1 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an
2 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or
3 endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the
4 entities, materials, or equipment are necessarily the best available for the purpose.

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

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

14 **NIST Technical Series Policies**

15 [Copyright, Fair Use, and Licensing Statements](#)

16 [NIST Technical Series Publication Identifier Syntax](#)

17 **How to Cite this NIST Technical Series Publication:**

18 Keller N, Quinn S, Scarfone, K, Smith M, Johnson V (2022) National Online Informative References (OLIR)
19 Program: Overview, Benefits, and Use. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
20 Interagency or Internal Report (IR) NIST IR 8278r1 ipd. <https://doi.org/10.6028/NIST.IR.8278r1.ipd>

21 **Author ORCID iDs**

22 Nicole Keller: 0000-0003-4761-6817

23 Stephen Quinn: 0000-0003-1436-684X

24 Karen Scarfone: 0000-0001-6334-9486

25 Matthew C. Smith: 0000-0003-1004-7171

26 Vincent Johnson: 0000-0002-7363-996X

27 **Public Comment Period**

28 December 8, 2022 – January 20, 2023

29 **Submit Comments**

30 olir@nist.gov

31

32 National Institute of Standards and Technology

33 Attn: Computer Security Division, Information Technology Laboratory

34 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

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

36 **Abstract**

37 Information and communication technology (ICT) domains – such as cybersecurity, privacy, and
38 Internet of Things (IoT) – have many requirements and recommendations made by national and
39 international standards, guidelines, frameworks, and regulations. An Online Informative
40 Reference (OLIR) provides a standardized expression of the relationships between concepts in
41 such documents. OLIRs provide a consistent and authoritative way of specifying relationships
42 that can be used by both humans and automation. The National OLIR Program is a NIST effort
43 to encourage and facilitate subject matter experts in defining OLIRs and to provide a centralized
44 location for displaying and comparing OLIRs. This report provides an overview of the National
45 OLIR Program, explains the basics of OLIRs and the benefits they can provide, and shows how
46 anyone can access and use OLIRs.

47 **Keywords**

48 catalog; crosswalk; informative references; mapping; National OLIR Program; Online
49 Informative References (OLIRs).

50 **Reports on Computer Systems Technology**

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

59 **Audience**

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

63 **Acknowledgments**

64 Thanks to all of those who contributed to or commented on this document, particularly Murugiah
65 Souppaya from NIST.

66 **Trademark Information**

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

68 **Call for Patent Claims**

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

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

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

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

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

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

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

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

93 Such statements should be addressed to: olir@nist.gov

94	Table of Contents	
95	1 Introduction	1
96	1.1 Purpose and Scope	2
97	1.2 Document Structure	2
98	2 OLIR Overview	3
99	2.1 Understanding Relationships	4
100	2.1.1 Relationship Rationales	4
101	2.1.2 Relationship Types	5
102	2.1.3 Relationship Strength	8
103	2.2 Reference Data in the OLIR Catalog	9
104	2.2.1 OLIRs	9
105	2.2.2 Derived Relationship Mappings (DRMs)	10
106	2.3 NIST Cybersecurity and Privacy Reference Tool (CPRT)	12
107	3 Using the OLIR Catalog	13
108	3.1 Searching the OLIR Catalog	13
109	3.2 Using the DRM Analysis Tool	18
110	3.3 Generating a Display Report	19
111	3.4 Downloading a Report	21
112	3.5 Inferring Additional Relationships Between Reference Documents	23
113	References	25
114	Appendix A. List of Symbols, Abbreviations, and Acronyms	26
115	Appendix B. Glossary	27
116	Appendix C. Change Log	28
117	List of Tables	
118	Table 1. Relationship Type Descriptions	5
119	Table 2. OLIR More Details Description Fields	14
120	Table 3. Display Report Column Header Descriptions	21
121	List of Figures	
122	Fig. 1. Relationship Types	5
123	Fig. 2. Example of Subset Relationship	6
124	Fig. 3. Example of Intersects Relationship	6
125	Fig. 4. Example of Equal Relationship	7
126	Fig. 5. Example of Superset Relationship	7
127	Fig. 6. Example of Unrelated Concepts	8
128	Fig. 7. Relative Strength of Relationships	9
129	Fig. 8. Multiple Documents Related to a Focal Document	11
130	Fig. 9. OLIR More Details Page	14

131	Fig. 10. OLIR Catalog Page	17
132	Fig. 11. DRM Analysis Tool Home Page	18
133	Fig. 12. Multi-Select Example	19
134	Fig. 13. Display Report Example	20
135	Fig. 14. Report Download Options	21
136	Fig. 15. Sample CSV Report	22
137	Fig. 16. Sample JSON Report	22
138		

139 **1 Introduction**

140 Information and communication technology (ICT) domains – such as cybersecurity, privacy, and
141 the Internet of Things (IoT) – have many requirements and recommendations made by national
142 and international standards, guidelines, frameworks, and regulations. Your organization
143 determines which standards, guidelines, frameworks, and regulations it *must* follow as well as
144 what it *chooses* to follow. Each of these documents has a unique set of requirements and
145 recommendations, and each document creator typically organizes and presents their content in
146 whatever prose format and structure they find suitable.

147 You and your colleagues need to identify all of the applicable requirements and
148 recommendations across all of these documents and make sense of them as a whole. Here are
149 some notional examples of what you might need to know:

- 150 • Implementing new security control X would help satisfy particular requirements and
151 recommendations in four documents.
- 152 • You need to update your remote access policy to include a requirement from document
153 A. That requirement is more stringent than what the other documents state, so updating
154 the policy to include what document A needs should help address the corresponding
155 items in the other documents.
- 156 • Your organization needs to comply with a new standard, so you need to determine which
157 of its requirements you already meet, which you do not meet, and which potentially
158 conflict with other requirements that you are subject to.

159 Knowing these things involves identifying the relationships between the items in the documents.
160 Figuring that out yourself is usually time-consuming and prone to error, especially because you
161 are unlikely to be an expert on the documents. Some documents include crosswalks, which
162 provide basic information about which items in one document may relate to items in another
163 document. For example, the NIST Cybersecurity Framework [1] adopted the term *Informative*
164 *References* for its crosswalks; each Informative Reference indicates one or more parts of another
165 document where readers can find additional information on the topic. Within the context of this
166 document (and the National OLIR Program), a *crosswalk* indicates that a relationship exists
167 between two items without any additional characterization of that relationship.

168 In a general sense, a mapping indicates how items of one document relate to items of another
169 document. However, within the context of this document and the National OLIR Program,
170 a *mapping* indicates the relationships between elements (items) of two documents by both
171 qualifying the rationale for indicating the connection between elements (semantic, syntactic, or
172 functional) and classifying the relationship utilizing set theory principles (subset of, intersects
173 with, equal, superset of, not related to).

174 An *Online Informative Reference (OLIR)* records the relationships between elements of two
175 documents as either a crosswalk (a *crosswalk OLIR*) or a mapping (a *mapping OLIR*) in
176 accordance with the OLIR specification. OLIRs are consistent, authoritative, and standardized
177 expressions of relationships that can be used by both humans and automation. Automated
178 approaches are necessary because of the ever-expanding pool of documents. Defining OLIRs
179 outside of the documents themselves also facilitates updating the OLIRs as needed instead of

180 having to wait until a document containing OLIRs is updated and re-released. Future NIST
181 publications are likely to use OLIRs instead of documenting relationships in an ad hoc manner
182 within the publications themselves.

183 Each OLIR is formatted according to a simple standard defined by NIST Interagency or Internal
184 Report (IR) 8278A, Revision 1, *National Online Informative References (OLIR) Program:
185 Submission Guidance for OLIR Developers* [2], and is displayed in a centralized location – the
186 OLIR Catalog. The OLIR Catalog is publicly accessible, so you can use it to access, view, and
187 download OLIRs for various pairs of documents.

188 **1.1 Purpose and Scope**

189 The purpose of this document is to introduce the National OLIR Program, highlight the benefits
190 of OLIRs, and explain what OLIRs are and how to use the OLIR Catalog.

191 After reading this document, any subject matter experts (SMEs) interested in creating content for
192 the OLIR Catalog should also read NIST IR 8278A, Revision 1 [2], which provides information
193 on defining OLIRs and submitting them to the Program.

194 **1.2 Document Structure**

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

- 196 • Section 2 provides an overview of OLIR and the OLIR Catalog.
- 197 • Section 3 describes common uses of the OLIR Catalog.
- 198 • The References section lists the references cited in this publication.
- 199 • Appendix A contains a list of the acronyms used throughout this document.
- 200 • Appendix B provides a glossary of terminology used throughout this document.
- 201 • Appendix C offers a brief change log for this revision of the document.

202 **2 OLIR Overview**

203 The National OLIR Program is a NIST effort to provide a single online location – the OLIR
204 Catalog – for displaying and comparing OLIRs for ICT domain documents. The Program uses
205 the terms *OLIR*, *Informative Reference*, and *Reference* interchangeably. The Program defines a
206 simple format in NIST IR 8278A [2] for expressing OLIRs in a standardized and consistent
207 manner.

208 As part of the Program, NIST experts are defining OLIRs between NIST documents, such as:

- 209 • Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity
210 Framework) version 1.1 [1]
- 211 • Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management
212 (Privacy Framework) version 1.0 [3]
- 213 • NIST IR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [4]
- 214 • Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for*
215 *Information Systems and Organizations* [5]

216 The Program also facilitates third parties in defining OLIRs between a document that they
217 created or for which they are an SME and a document that is already represented in the OLIR
218 Catalog. Creators of OLIRs are known as *OLIR Developers*, or simply *Developers*. The National
219 OLIR Program defines a formal process for Developers to submit OLIRs to NIST [2]. This
220 process includes guidance for creating high-quality, more usable, better-documented OLIRs. It
221 also defines a managed process for reviewing, updating, and maintaining OLIRs as the
222 documents they are based on are revised and updated. NIST encourages document owners,
223 software vendors, service providers, educators, and other parties to develop and submit OLIRs to
224 the National OLIR Program.

225 The National OLIR Program offers several benefits to anyone working with cybersecurity,
226 privacy, or other information and communications technology domain documents, including the
227 following:

- 228 • The OLIR Catalog is a single, easy-to-use repository where you can obtain information
229 on many documents and analyze their relationships. OLIRs provide a much more cost-
230 effective method for you and others to establish and verify the relationships between the
231 documents you use.
- 232 • Standardizing how relationships are expressed makes them more consistent, clear, usable,
233 repeatable, and organizable, and it provides a way for automation technologies to ingest
234 and utilize them.
- 235 • The National OLIR Program authenticates the source of each OLIR and allows you to
236 identify who provided each OLIR.
- 237 • The National OLIR Program helps facilitate the integration of NIST guidance, which is
238 produced in support of United States Government (USG) legislative and administrative
239 responsibilities.

240 Note that although using OLIRs can significantly improve understanding of documents within
241 organizations, it does not demonstrate or certify that an organization complies with a document.
242 It can, however, assist in that process.

243 **2.1 Understanding Relationships**

244 Every OLIR compares elements of two documents and characterizes their relationship. The first
245 document, called the *Focal Document*, is used as the basis for the comparison. All Focal
246 Documents are NIST publications. The second document is called the *Reference Document*. Note
247 that a Focal Document or a Reference Document is not necessarily in a traditional document
248 format (e.g., a formal publication in a PDF) but could be a product, service, training, or other
249 content. A *Focal Document Element* or a *Reference Document Element* is a discrete section,
250 sentence, phrase, or other identifiable piece of content from a document.

251 Each crosswalk OLIR indicates pairs of Focal Document Elements and Reference Document
252 Elements that have relationships. Each mapping OLIR does that as well but also characterizes
253 each element-to-element relationship by its rationale, type, completeness, and (optionally)
254 strength. Each of these is discussed in the following subsections. People already implicitly
255 identify these characteristics but are not aware of doing so. One of the goals of the National
256 OLIR Program is to elucidate the science by encouraging explicit declarations of OLIR
257 relationship characteristics.

258 **2.1.1 Relationship Rationales**

259 The basic reason why a Reference Document Element and a Focal Document Element are related
260 is attributed to one of three *rationales*:

261 1. **Syntactic** – Compares the **linguistic meaning** of the two elements. For example, the
262 following statements have the same syntax:

```
263 printf ("bar"); [... C programming language]  
264 printf ("bar"); [... C programming language]
```

265 2. **Semantic** – Compares the **contextual meaning** of the two elements. For example, the
266 following statements convey the same semantic meaning:

267 “The organization employs a firewall at the network perimeter.”

268 “The enterprise uses a device that has a network protection application installed to
269 safeguard the network from intentional or unintentional intrusion.”

270 3. **Functional** – Compares the **functions** of the two elements. For example, the following
271 statements have the same functional result:

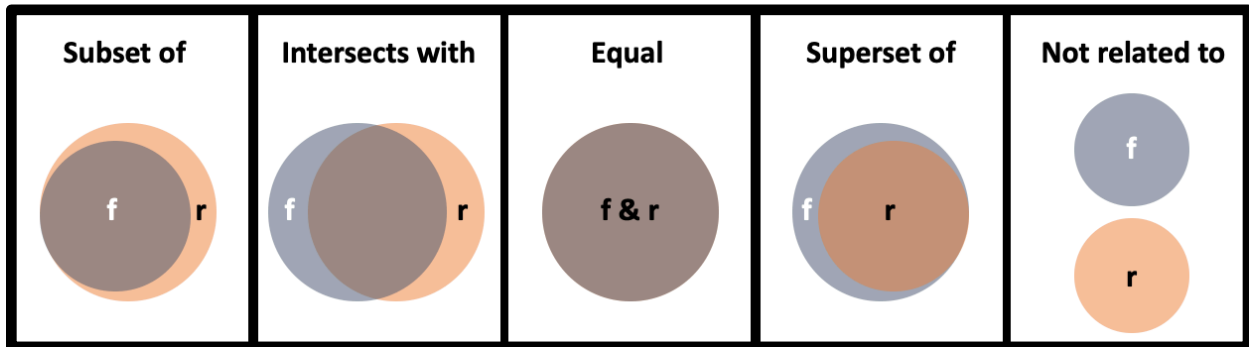
```
272 printf ("foo\n"); [... C programming language]  
273 print "foo" [... BASIC programming language]
```

274 Each of these examples has two statements that could be considered equal **within the scope of**
275 **the rationale**. While the statements in the last example may be functionally equivalent, they are
276 not semantically equivalent because they describe different ways to achieve the same
277 functionality, and they are of course not syntactically equivalent because their wordings are

278 much different. Most relationships captured by OLIRs are not of equal or equivalent statements.
279 The next subsection examines this in more detail.

280 **2.1.2 Relationship Types**

281 Each relationship between a Focal Document Element and a Reference Document Element is
282 classified by a *relationship type*. The relationship type indicates how the meanings of the two
283 elements are related within the context of a particular rationale (e.g., syntactic, semantic, or
284 functional). For each relationship, the relationship type will be one of the following, as depicted
285 in Figure 1 (where “f” is a Focal Document Element and “r” is a Reference Document Element)
286 and further explained in Table 1.



287

288 **Fig. 1.** Relationship Types

288

289 **Table 1.** Relationship Type Descriptions

289

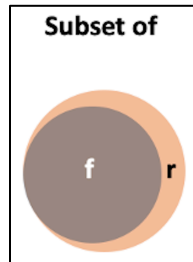
Relationship Type	Description
Subset of	The Focal Document Element is a subset of the Reference Document Element. In other words, the Reference Document Element contains everything that the Focal Document Element does and more.
Intersects with	The two elements have some overlap, but each includes content that the other does not.
Equal	The two elements are very similar though not necessarily identical.
Superset of	The Focal Document Element is a superset of the Reference Document Element. In other words, the Focal Document Element contains everything that the Reference Document Element does and more.
Not related to	The two elements do not have anything in common.

290

291 Relationship types have a natural order: Equal, Subset and Superset, Intersects with, and Not
292 Related. The Equal type indicates the most in common between the elements, and Not Related
293 assertions indicate nothing in common.

294 The examples below illustrate each of the five relationship types. The Reference Document
295 Elements are from NIST SP 800-171, and the Focal Document Elements are from version 1.1 of
296 the Cybersecurity Framework.

297 **Example 1: Subset**



298

299

Fig. 2. Example of Subset Relationship

300

301

- Focal Document Element: PR.AT-4, “Senior executives understand their roles and responsibilities.”

302

303

304

- Reference Document Element: Requirement 3.2.2, “Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.”

305

306

307

308

309

The OLIR Developer selects the functional rationale for this relationship. PR.AT-4 states that a specific group of users (senior executives) should be trained on their roles and responsibilities. Requirement 3.2.2 states that “all users” should be trained on their roles and responsibilities. The Developer asserts that the concept “all users” contains the concept “senior executives and others.”

310

311

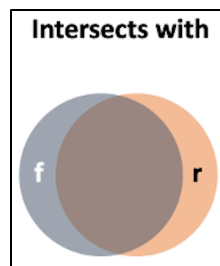
312

313

Because PR.AT-4 is one part of requirement 3.2.2, and PR.AT-4 does not contain any concepts that requirement 3.2.2 does not contain, the relationship type is Subset. In other words, PR.AT-4 (the Focal Document Element) is a subset of requirement 3.2.2 (the Reference Document Element).

314

Example 2: Intersects with



315

316

Fig. 3. Example of Intersects Relationship

317

318

- Focal Document Element: RS.CO-2, “Incidents are reported consistent with established criteria.”

319

320

- Reference Document Element: Requirement 3.6.2, “Track, document, and report incidents to appropriate organizational officials and/or authorities.”

321

322

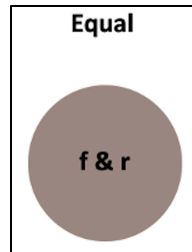
323

324

The OLIR Developer selects the semantic rationale for this relationship. Both RS.CO-2 and requirement 3.6.2 address the same concept of documenting and reporting incidents. However, RS.CO-2 contains the concept of “established criteria,” and requirement 3.6.2 contains the concept of “appropriate organizational officials and authorities.”

325 Because the two elements address the same concept, but each element also includes an additional
326 concept that the other does not include, the relationship type is Intersects with. In other words,
327 RS.CO-2 (the Focal Document Element) intersects with requirement 3.6.2 (the Reference
328 Document Element).

329 **Example 3: Equal**



330

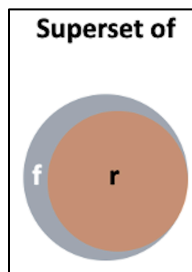
331 **Fig. 4.** Example of Equal Relationship

- 332
- Focal Document Element: PR.PT-3, “The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.”
 - Reference Document Element: Requirement 3.4.6, “Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.”
- 334
- 335
- 336

337 The OLIR Developer could select either functional or semantic as the rationale for this
338 relationship. Both PR.PT-3 and requirement 3.4.6 communicate the concept of
339 “employing/incorporating the principle of least functionality by configuring systems to provide
340 only essential capabilities.” Neither PR.PT-3 nor requirement 3.4.6 contains any concepts that
341 the other does not.

342 Because the two elements say the same thing, the relationship type is Equal. In other words,
343 PR.PT-3 (the Focal Document Element) is equal to requirement 3.4.6 (the Reference Document
344 Element).

345 **Example 4: Superset of**



346

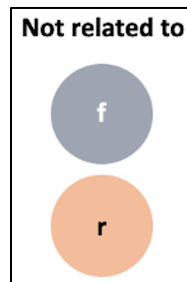
347 **Fig. 5.** Example of Superset Relationship

- 348
- Focal Document Element: PR.AC-1, “Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.”
 - Reference Document Element: Requirement 3.5.1, “Identify system users, processes acting on behalf of users, and devices.”
- 350
- 351

352 The Developer selects functional as the rationale for this relationship. PR.AC-1 includes several
353 concepts for device, user, and process identities and credentials, including issuing, managing,
354 verifying, revoking, and auditing them. Requirement 3.5.1 is about identifying devices, users,
355 and processes, which is needed for PR.AC-1. However, requirement 3.5.1 does not include any
356 of the other parts of PR.AC-1.

357 Because requirement 3.5.1 is one part of PR.AC-1, and requirement 3.5.1 does not contain any
358 concepts that PR.AC-1 does not contain, the relationship type is Superset. In other words,
359 PR.AC-1 (the Focal Document Element) is a superset of requirement 3.5.1 (the Reference
360 Document Element).

361 **Example 5: Not related to**



362

363

Fig. 6. Example of Unrelated Concepts

364 This relationship type is used when the Focal Document Element and the Reference Document
365 Element do not share any concepts. In OLIRs submitted to the OLIR Catalog, Reference
366 Document Elements that do not relate to any Focal Document Elements are either marked as
367 “not related to” or omitted altogether.

368 **2.1.3 Relationship Strength**

369 The National OLIR Program provides a means for an OLIR Developer to subjectively quantify
370 the strength of a relationship between elements. This metric can provide additional insight for the
371 implied bond between elements asserted by the Developer. Figure 7 illustrates how a single
372 relationship type can encompass relationships of different strengths. For example, Case 1 shows
373 a Focal Document Element and a Reference Document Element in a Subset relationship with
374 much in common, while Case 2 shows a Subset relationship where the two elements have
375 relatively little in common. The other pairs of cases each depict different strengths of the same
376 relationship type.

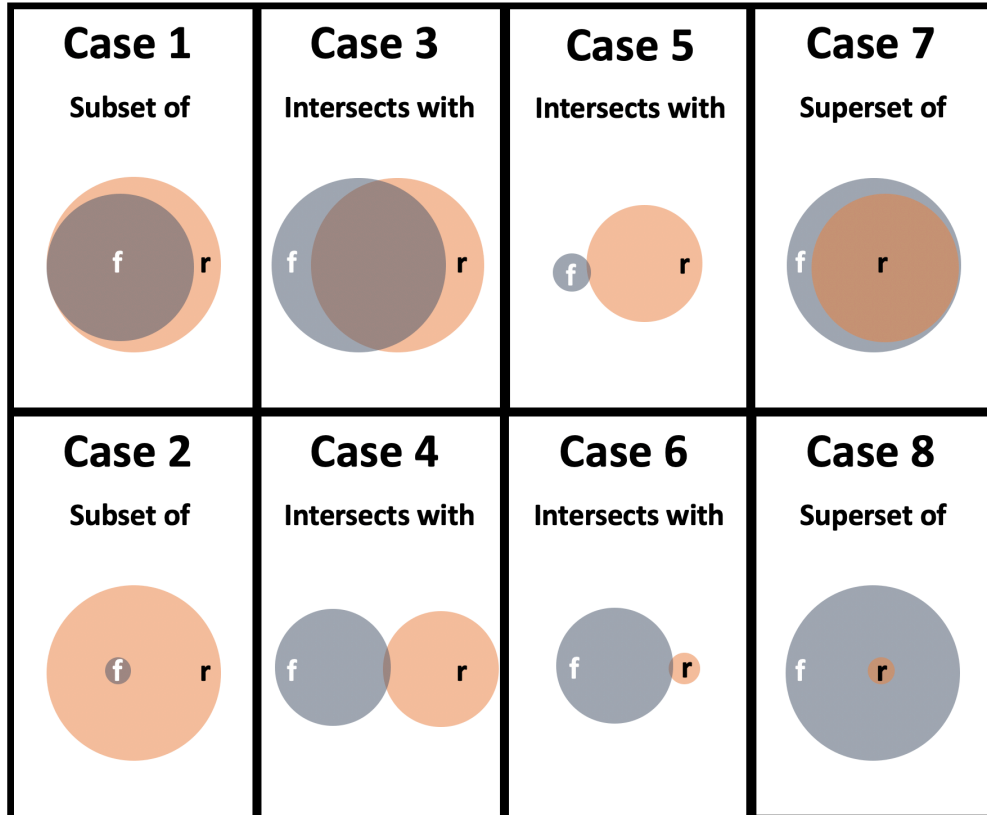


Fig. 7. Relative Strength of Relationships

377

378

379 The Program encourages OLIR Developers to include a measure of the strength of comparable
380 relationships but does not prescribe a methodology for doing so. Quantifying the strength of a
381 relationship is optional, and its omission should not be interpreted as negative. It is intended for
382 lateral comparisons, like the Cybersecurity Framework and the Privacy Framework, and not
383 comparisons of documents at vastly different levels of abstraction, such as the Cybersecurity
384 Framework and a research paper on a topic in quantum cryptography. The strength of non-lateral
385 relationships is designated with “N/A.”

386 2.2 Reference Data in the OLIR Catalog

387 The OLIR Catalog contains information on two types of relationships between Focal Documents
388 and Reference Documents: OLIRs and Derived Relationship Mappings. These relationships are
389 organized as *Reference Data* via the OLIR Catalog.

390 2.2.1 OLIRs

391 OLIRs have been vetted by NIST to ensure compliance with the NIST IR 8278A specification,
392 submitted for a public comment period, and finalized. The National OLIR Program has two
393 major source types for OLIRs:

- 394 1. **Owner:** These are produced by the owner of the Reference Document. For example,
395 NIST is the owner of NIST SP 800-171 [6] and produced the OLIR for SP 800-171.

396 Therefore, the designation of “owner” is granted to the SP 800-171 OLIR developed by
397 NIST.

398 2. **Non-Owner:** These are produced by an SME other than the Reference Document owner.

399 Each OLIR is also categorized as either unilateral or bilateral, depending on which individuals or
400 organizations created or validated it:

- 401 • **Unilateral:** NIST is not the owner of the Reference Document. The OLIR was created by
402 a third party, and NIST has not validated the assertions made by the OLIR’s Developer.
- 403 • **Bilateral:** NIST is the owner of the Reference Document. Either NIST has developed the
404 OLIR (owner-produced OLIR), or a third party has developed the OLIR (non-owner-
405 produced OLIR) and NIST has validated its assertions and reached agreement with the
406 developer.

407 When multiple OLIRs are available for a particular Focal Document/Reference Document pair,
408 consider the following:

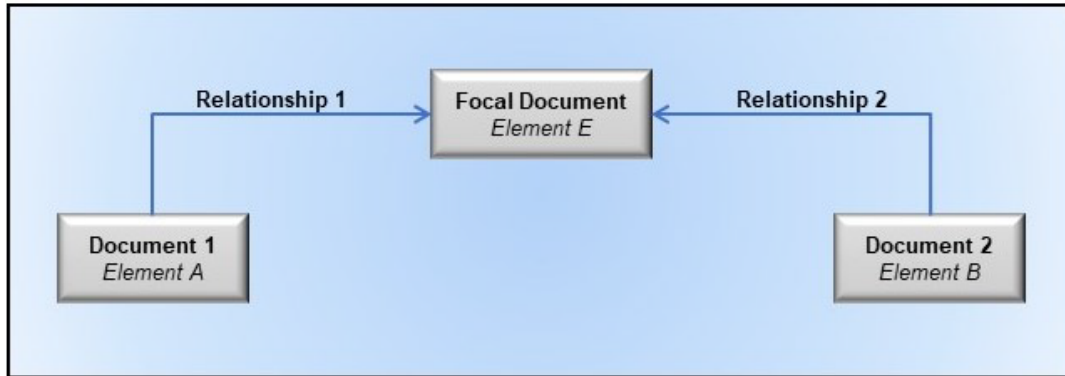
- 409 • Generally, bilateral OLIRs should be favored over unilateral OLIRs.
- 410 • Generally, owner-produced OLIRs should be favored over non-owner-produced OLIRs.
- 411 • Generally, mapping OLIRs should be favored over crosswalk OLIRs.

412 If it is not clear which OLIR should be analyzed, focus on the quality and completeness of the
413 OLIRs.

414 **2.2.2 Derived Relationship Mappings (DRMs)**

415 If OLIRs are not available for a particular Focal Document/Reference Document pair, you may
416 be able to glean some of the mappings by using the OLIR Catalog’s Derived Relationship
417 Mappings (DRM) tool. DRMs are the result of using the OLIRs between two Reference
418 Documents and a single Focal Document to make inferences about relationships between the two
419 Reference Documents. Every OLIR submission uses standard identifiers for the Focal Document
420 Elements, and these standard identifiers make it possible to associate Reference Document
421 Elements with each other through their relationships to a common Focal Document Element.
422 DRMs are dynamically generated when you use the DRM Analysis Tool to search the OLIR
423 Catalog. The results of the search are displayed to you, as Section 3.2 shows.

424 DRMs serve as the foundation for gap and comparative analysis. Figure 8 depicts how you could
425 look for a relationship between Reference Document 1–Element A and Reference Document 2–
426 Element B based on their individual relationships to Focal Document–Element E. DRMs do not
427 indicate the relationships between the Reference Documents. Therefore, in reference to Figure 8,
428 if an organization implements Document 1–Element A, that does not necessarily mean it is also
429 implementing Document 2–Element B. The two elements are *potentially* related. Even when the
430 relationship is “equal,” that does not mean the two elements are identical and does not imply that
431 implementing one element means compliance with the other element.



432

433

Fig. 8. Multiple Documents Related to a Focal Document

434 Another caveat about DRMs is that the elements being compared are often at different levels of
435 detail (sometimes referred to as “different levels of abstraction”). For example, suppose you
436 want to compare Element PR.AC-1, “Identities and credentials are issued, managed, verified,
437 revoked, and audited for authorized devices, users, and processes” [1], to Element IA-7,
438 “Cryptographic Module Authentication,” which is defined as “The information system
439 implements mechanisms for authentication to a cryptographic module that meet the requirements
440 of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and
441 guidance for such authentication” [5]. PR.AC-1 is at a higher level than IA-7, which specifies, in
442 detail, one part of what PR.AC-1 encompasses. For some DRMs, the difference in the level of
443 detail of the elements being compared may be vast.

444 Before the National OLIR Program, analyzing documents often meant you would have to
445 conduct a manual comparison, perhaps by copying the contents of both documents into a
446 spreadsheet for easier searching and sorting. You would then likely resort to using section
447 headers as a starting point for the comparison because of a lack of consistent identifiers within
448 the documents. For example, if you were comparing the Cybersecurity Framework with NIST SP
449 800-171 [6], you could start within the Cybersecurity Framework Reference Document at the
450 “Asset Management (ID.AM) Category,” then proceed to SP 800-171 and find a section where
451 an element similar to the Cybersecurity Framework element might be documented. For this
452 example, you might select Section 3.4, “Configuration Management,” of SP 800-171 and read
453 through each of its basic and derived security requirements to identify relationships. You would
454 repeat this laborious and error-prone process for all of the Categories and Subcategories within
455 the Cybersecurity Framework and all of the basic and derived requirements of SP 800-171.
456 Multiply this process by other people also finding the relationships, and two problems quickly
457 emerge: 1) the different opinions of people result in inconsistent associations, and 2) an
458 enormous amount of effort is duplicated. Streamlining this process is the main reason the OLIR
459 DRM capability was created.

460 To save time, you can utilize DRMs. For example, you could leverage the OLIRs for Reference
461 Document SP 800-171 to Focal Document SP 800-53 [5] and the OLIRs for Reference
462 Document Cybersecurity Framework to Focal Document SP 800-53. SP 800-53 would serve as a
463 transitive link for identifying commonality between the Cybersecurity Framework and SP 800-
464 171. SP 800-171 Requirement 3.4.1 lists a relationship with SP 800-53 control CM-8. After you
465 search the Cybersecurity Framework Core for mappings to CM-8, you see there is a relationship

466 listed for subcategories ID.AM-1, ID.AM-2, PR.DS-3, and DE.CM-7. You could then focus your
467 comparative analysis on these elements.

468 Though the inferences that you may make while using DRMs are informative, **they are not**
469 **considered verified nor authoritative**. DRMs can help you make better-informed decisions
470 regarding risk management, compliance, control selection, and solution implementation
471 activities, but they are only intended to aid you in conducting your own analysis, not to take the
472 place of analysis.

473 **2.3 NIST Cybersecurity and Privacy Reference Tool (CPRT)**

474 The NIST Cybersecurity and Privacy Reference Tool (CPRT) is a separate effort from OLIR,
475 though it is a closely related and complementary resource. CPRT offers a consistent format for
476 accessing reference data from selected NIST cybersecurity and privacy standards, guidelines,
477 and frameworks in a unified data format. These datasets, which include several of the OLIR
478 Focal Documents, will make it much easier for users to identify, locate, compare, and customize
479 content in and across NIST resources without needing to review hundreds of pages of narrative
480 within the publications. The reference data can be exported in different data formats, including a
481 machine-readable JavaScript Object Notation (JSON) format.

482 The CPRT project is in its initial phase as of this writing. For more information on CPRT and its
483 future phases, visit <https://csrc.nist.gov/Projects/cprt>.

484 **3 Using the OLIR Catalog**

485 This section provides information on how you can use the OLIR Catalog. Section 3.1 reviews the
486 interfaces for viewing and searching the OLIRs in the Catalog, as well as the supporting
487 information that the Catalog holds for each OLIR. Section 3.2 provides information on the DRM
488 Analysis Tool that helps characterize relationships between Reference Documents. Section 3.3
489 explains how to generate on-screen reports between OLIRs, and Section 3.4 discusses how to
490 download reports in multiple formats. Finally, Section 3.5 explores an additional use case for the
491 OLIR Catalog: inferring additional relationships between Reference Documents based on
492 authoritative OLIRs.

493 **3.1 Searching the OLIR Catalog**

494 The OLIR Catalog¹ contains all of the Reference Data – OLIR data and DRMs – for the National
495 OLIR Program. All Reference Data in the OLIR Catalog has been validated against the
496 requirements of NIST IR 8278A [2] and is displayed according to the most recent OLIR
497 received. The OLIR Catalog provides an interface for viewing OLIRs and analyzing Reference
498 Data.

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

503 Selecting the “More Details” link of an OLIR in the Catalog will display a description page,
504 shown in Figure 9, that includes the General Information of an OLIR.

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

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

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

IR JSON

[NIST-Cybersecurity-Framework-Informative-Reference-for-800-171-Rev-1.json](#)

SHA-256
CF13915681B965DF94835B506E9B25A79D7BF0F1D05B616EC65EC7037428CADE

505

506

Fig. 9. OLIR More Details Page

507

Table 2 lists fields and descriptions of the information depicted on the More Details page in Figure 9.

508

509

Table 2. OLIR More Details Description Fields

Field Name	Description
Informative Reference Name	The name by which the OLIR 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
Web Address	The URL where the OLIR can be found

Field Name	Description
Status	<p>Indicates the current status of the OLIR:</p> <ul style="list-style-type: none"> • Work-in-progress draft: It is currently in an early stage of development and is incomplete. It has not been extensively edited or vetted. Work-in-progress drafts are solely informational in nature and are not intended to be implemented. • Preliminary draft: It is considered stable, but changes are expected to occur. There are gaps in the content, and the document is still incomplete. Early adopters may consider experimenting with the content with the understanding that they will identify gaps and challenges. • Draft: It is a complete draft proposed as a candidate for Final status. Changes may occur based on public comments, but such changes are expected to be relatively minor. Early adopters may attempt to use the content. • Final: Comments from the public comment period have been addressed, and the Informative Reference has been published as final.
Informative Reference Version	The version of the OLIR 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 OLIR
Summary	The purpose of the OLIR
Target Audience	The intended audience for the OLIR
Comprehensive	Whether the OLIR 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/or phone number within the OLIR Developer’s organization
Category of Submitter	<p>The category type of the OLIR:</p> <ul style="list-style-type: none"> • Public sector: A governmental or regulatory agency, bureau, or board of the United States (federal, state, local) • Private sector: Any incorporated group that provides products, services, or information that cover topics related to the Focal Document • Academia: Informative references that originate from educational institutions, such as universities, colleges, and research laboratories • Other: Informative references that do not fall into the previous categories, such as standards development organizations and international governments
Citations	A list of source material (beyond the Reference Document) that supported development of the OLIR
SHA3-256	The hash value checksum that is generated between the validated OLIR sent to the OLIR Program and the publicly available OLIR. The value is monitored to maintain data integrity of the OLIR.
Authority	The organization responsible for authoring the OLIR in relation to the organization that produced the Reference Document represented by the OLIR 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 OLIR

Field Name	Description
Posted Date	The date that a validated OLIR 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

510
511 Figure 10 shows the OLIR Catalog Page where you can browse and search for OLIR content in
512 multiple ways. You can search the entire OLIR Catalog to locate and retrieve an OLIR using a
513 variety of fields, such as Informative Reference Name, Reference Document, Posted Date,
514 Status, and Submitting Organization. Utilizing the dropdowns in the *Advanced Search* section,
515 you can search OLIRs based on a Focal Document of your choice. You can also locate and
516 retrieve an OLIR using a variety of fields, such as the type of Authority or Category of Submitter
517 that an OLIR is cataloged as. Additionally, you can perform keyword searches of catalog content
518 and sort the catalog columns within the table in a variety of different ways.

[Derived Relationship Mapping](#)

ADVANCED SEARCH

Focal Document Cybersecurity Framework v1.1

Informative Reference Name

Reference Document

Posted Date // to //

Authority Non-Owner Owner

Category of Submitter Academia Other Private Sector Public Sector

Keyword(s)

Status

Sort By Status (A-Z)

Search **Reset**

Showing 1 through 10 of 20 matching records. 1 | 2 > >>

Status	Informative Reference (version)	Reference Document	Posted Date	Focal Document	Submitting Organization	Authority	Category of Submitter
Final	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	Cybersecurity Framework v1.1	NIST	Owner	Public Sector
Final	HITRUST-CSF-v9-2-to-NIST-CSF-v1-1 (1.0.0) (More Details)	HITRUST CSF v9.2	11/19/19	Cybersecurity Framework v1.1	HITRUST Alliance; Standards	Owner	Private Sector

Fig. 10. OLIR Catalog Page

520 3.2 Using the DRM Analysis Tool

521 The DRM Analysis Tool² allows to generate DRMs for Reference Documents with a Focal
522 Document of your choice. The DRMs are non-authoritative and represent a starting point when
523 attempting to compare Reference Documents. Figure 11 depicts the homepage of the DRM
524 Analysis Tool.

Derived Relationship Mapping

The Derived Relationship Mapping (DRMs) Analysis Tool provides Users the ability to generate DRMs for Reference Documents with a Focal Document of the Users' choice. The DRMs are non-authoritative and represent a starting point when attempting to compare Reference Documents. Refer to Sections 3.3 – 3.6 of [NISTIR 8278, National Online Informative References \(OLIR\) Program: Program Overview and OLIR Uses](#), for additional guidance around understanding and utilizing the tool.

After creating a Display Report, Users can download the report in either a comma-separated value (CSV) file format or a JavaScript Object Notation (JSON) file format.

If interested in participating in the OLIR program, please refer to the [Informative Reference submission](#) page. To access the current list of Focal Document submission templates, please refer to the [Focal Document Templates](#) page.

To view the [JSON schema](#), [click here](#).

Generate Report

Focal Document Cybersecurity Framework v1.1

Informative Reference 1

Informative Reference 2

Informative Reference 3

Informative Reference 4

Function* ID, PR, DE, RS, RC

Category*

Subcategory*

* - Ctrl + Left Mouse Click to select multiple

Rationale Semantic, Syntactic, Functional

Relationship subset of, not related to, superset of, equal, intersects with

Strength* N/A, 0, 1, 2, 3, 4

Generate **Reset**

525
526 **Fig. 11. DRM Analysis Tool Home Page**

527 As Figure 11 shows, when accessing the DRM Analysis tool, you first select the Focal
528 Document for comparative analysis. Only Focal Documents with two or more OLIRs in the
529 OLIR Catalog are selectable in the Focal Document drop-down box. You can display potential
530 relationships for up to four OLIRs at a time for a given Focal Document. For example, you can
531 generate reports at any level of the Cybersecurity Framework Focal Document (i.e., Function,
532 Category, Subcategory) or the SP 800-53 Focal Document (i.e., Control Family, Security/Privacy
533 Control, Security Control Enhancements).

534 When you access this page, all rationale and relationship pairings (except for the “not related to”
535 relationship) are pre-selected by default. To filter out any rationale or relationship selections,
536 deselect checkboxes as appropriate before generating a report.

537 By default, the Strength of Relationship field is left unselected. You can generate reports with
538 this field unselected to display every type of strength defined within the OLIR of their search

² See <https://csrc.nist.gov/Projects/olir/derived-relationship-mapping>.

539 criteria. You can narrow your criteria by selecting a singular or multiple strength pairing for
540 further analysis.

541 In addition to performing an analysis at an individual level (i.e., selecting one Function,
542 Category, or Subcategory), you can also display OLIRs at multiple levels (i.e., selecting multiple
543 Functions, Categories, and Subcategories or multiple Control Families, Security/Privacy
544 Controls, or Security Control Enhancements). Figure 12 displays an example of multiple
545 Categories and Subcategories being selected for the Cybersecurity Framework Focal Document.
546 In this example, the two displayed Categories are ID.AM and ID.BE along with Subcategories
547 ID.AM-6 and ID.BE-1. The Strength of Relationship field has been left unselected.

548 To achieve this desired output, you should first select the “Cybersecurity Framework v1.1” Focal
549 Document from the drop-down menu. Then choose the OLIRs for comparative analysis. Next,
550 select the “ID” Function, which will result in the applicable Categories being displayed in the
551 Category box. To select multiple Categories on a Windows computer, you can hold the “Ctrl”
552 key and click on the ID.AM and ID.BE Categories. On a macOS computer, you can hold the
553 “Command” key instead. Choosing both ID.AM and ID.BE will cause all of the Subcategories
554 within ID.AM and ID.BE to be displayed in the Subcategory box. You can continue this
555 selection 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, numbered 1 through 4. Menu 1 is set to "NIST Cybersecurity Framework Informative Reference for 800", menu 2 to "NIST-Privacy-Framework-v1-to-NIST-CSF-v1-1", and menus 3 and 4 are empty. The "Function*" dropdown is set to "ID", which has opened a list of options: ID, PR, DE, RS, and RC. The "Category*" dropdown is set to "ID.AM" and "ID.BE", which has opened a list of options: ID.AM, ID.BE, ID.GV, ID.RA, and ID.RM. The "Subcategory*" dropdown is set to "ID.AM-6" and "ID.BE-1", which has opened a list of options: ID.AM-5, ID.AM-6, ID.BE-1, ID.BE-2, and ID.BE-3. Below these dropdowns is a note: "* - 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", and "intersects with" (all checked); and "Strength*" with a dropdown menu set to "N/A" and options 0, 1, 2, 3, and 4. At the bottom right, there are "Generate" and "Reset" buttons.

556

557

Fig. 12. Multi-Select Example

558 3.3 Generating a Display Report

559 After selecting the “Generate” option (see Figure 12), you are presented with an on-screen output
560 table. Figure 13 shows the results of comparing two OLIRs at the individual PR.AC-2
561 Subcategory level with the Cybersecurity Framework Focal Document selected. This on-screen
562 output is the *Display Report*.

Report
 Jun 11, 2022 09:19:00
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, 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

563

564

Fig. 13. Display Report Example

565 Due to screen space limitations, the Display Report stacks the results according to the Focal
 566 Document element. For example, if Reference A has two relationship pairings to a given Focal
 567 Document element, and Reference B has two relationship pairings to the same Focal Document
 568 element, the two Reference A relationships will be displayed in rows 1 and 2, followed by
 569 Reference B’s relationships in rows 3 and 4, with the Focal Document element identifier in the
 570 leftmost column of all four rows.

571 Hover-over “Tool Tips” are provided with descriptions when you scroll the pointer over the
 572 column headers. Figure 13 shows an example of a Tool Tip when hovering above the “Reference
 573 Element Description” column header. Likewise, the Cybersecurity Framework Core definitions
 574 are displayed using the same Tool Tips behavior when you hover over the Focal Document
 575 Element identifier displayed in the leftmost column.

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

577

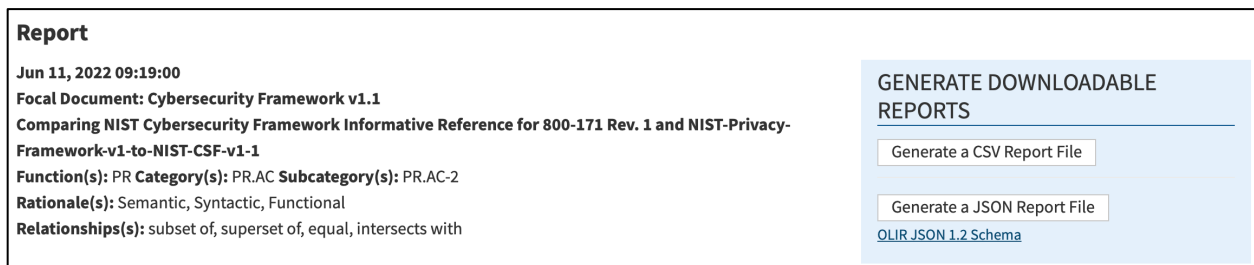
Table 3. Display Report Column Header Descriptions

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 for why a Reference Document Element and a Focal Document Element are related. This will be syntactic, semantic, or functional.
Relationship	The type of logical relationship that the OLIR Developer asserts the Reference Document Element has compared to the Focal Document Element. The Developer conducting the assertion should focus on the perceived intent of each of the Elements. This will be one of the following, as depicted in Figure 1: 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. For example, SP 800-53 control AC-13 may have been split into three pieces so that relationships can be identified for each piece. Each piece would have its own row in the Display Report, a unique Focal Document Identifier (e.g., AC-13:1, AC-13:2, AC-13:3), and the same Group identifier (e.g., AC-13).
Strength of Relationship	The extent to which a Reference Document Element and a Focal Document Element are similar

578 **3.4 Downloading a Report**

579 After creating a Display Report, multiple report download options are available, as depicted in
 580 the right corner of Figure 14. Within “Generate Downloadable Reports” are links for CSV
 581 (comma-separated values) and JSON report files.³ Clicking on a “Generate” link causes the
 582 corresponding report file format to be downloaded. The report downloads contain more
 583 information than the Display Report (e.g., Focal Document Element description) for more
 584 convenient human comparison and automated processing.⁴

585



586

Fig. 14. Report Download Options

³ The CSV and JSON download links are only available after the Display Report is generated.

⁴ See NIST IR 8278A [2] for additional field descriptions.

587 Figure 15 represents a sample CSV report. This is a common format that is easily ingested into a
588 spreadsheet program where searching and sorting functions can be performed. Those functions
589 are not available via the DRM Analysis Tool.

	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 Cybersecurity Framework 3.10.1	Semantic	superset of	Limit physical access	N/A			Limiting access	N/A		
3	PR.AC-2	Physical access	NIST Cybersecurity Framework 3.10.2	Semantic	intersects	Protect and defend	N/A				N/A		
4	PR.AC-2	Physical access	NIST Cybersecurity Framework 3.10.3	Functional	intersects	Escort visits	N/A				N/A		
5	PR.AC-2	Physical access	NIST Cybersecurity Framework 3.10.4	Functional	intersects	Maintain and monitor	N/A				N/A		
6	PR.AC-2	Physical access	NIST Cybersecurity Framework 3.10.5	Functional	superset of	Control and monitor	N/A			"Physical access"	N/A		
7	PR.AC-2	Physical access	NIST-Privacy Framework PR.AC-P2	Functional	superset of	Physical access	N/A				N/A		
8													

590

591

Fig. 15. Sample CSV Report

592 The JSON format provides the report data in a format that many tools can utilize to perform
593 more in-depth analyses that are not available using the DRM Analysis Tool. The JSON file
594 depicted in Figure 16 shows how the data is displayed.

```
{
  "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": ""
    }
  ],
}
```

595

596

Fig. 16. Sample JSON Report

597 **3.5 Inferring Additional Relationships Between Reference Documents**

598 The stacked Display Report and report download options provide a convenient way to quickly
599 view how one Reference Document may relate to another by leveraging a Focal Document that
600 they have in common. The DRM Analysis Tool automates the brute force comparison method
601 for analyzing Reference Documents and renders transitive relationship possibilities for the
602 analyst to consider. The DRM Analysis Tool output only displays authoritative relationships. If
603 you compare the relationships from different Reference Documents and infer additional
604 relationships among them, those inferred – *derived* – relationships are non-authoritative.
605 However, they are still useful because they represent a starting point for various types of
606 comparative analysis and research.

607 With much of the relationship data defined by the OLIR Developer already, you can simply
608 generate a full report between two Reference Documents by selecting all desired Rationale and
609 Relationship types and exporting the stacked data output in CSV format to import it into a
610 spreadsheet application for searching and sorting reference data. For example, once the CSV file
611 is imported, you can sort the reference data by Functions, Categories, and Subcategories or
612 Control Families, Security/Privacy Controls, or Security Control Enhancements (depending on
613 the Focal Document selected.) Then, using the Rationale and Relationship designations, you can
614 better understand the similarities and differences between the elements and determine which
615 relationships are relevant.

616 To narrow the potential for identifying strong associations between Reference Documents, you
617 could generate a Display Report using the Rationale and Relationship selectors to indicate
618 association strength. By selecting options such as “semantic” and “equal to,” you can parse the
619 Display report for Reference relationships that have a better chance of relevance than, for
620 example, what the options of “functional” and “intersection” might provide.

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

- 623 • If you know your organization already implements the NIST Privacy Framework, and
624 NIST publishes a new version of SP 800-171, you can generate a Display Report
625 selecting the “not related to” Relationship option. This report may contain data that is
626 unrelated to the NIST Cybersecurity Framework, but it does not preclude the data from
627 relating to other Reference Documents. Just because SP 800-171 and the Privacy
628 Framework have elements that do not map to the Cybersecurity Framework does not
629 mean that the two Reference Documents are unrelated to each other.
- 630 • You could generate Display Reports in order to identify significant changes between two
631 versions of the same document. First, you could report on the relationships between the
632 Privacy Framework and the current version of SP 800-171. Next, you could report on the
633 relationships between the Privacy Framework and a new draft revision of SP 800-171.
634 Finally, you could use a tool to compare those two reports and identify their differences.
- 635 • You could identify the gaps that would need to be addressed if your organization adopted
636 a new security framework by generating a Display Report comparing the Reference
637 Documents that the organization already complies with to the Reference Document for
638 the new security framework.

639 A final gap analysis example involves a vendor of cybersecurity products and services. Such a
640 vendor could generate a Display Report that shows which requirements from Reference
641 Documents their products and services help to address. This provides a starting point for
642 conducting additional analysis for each identified requirement to determine the strength of each
643 relationship.

644 As additional use cases are identified for using the OLIR Catalog, they will be added to this
645 section of the document.

646 **References**

- 647 [1] National Institute of Standards and Technology (2018) Framework for Improving Critical
648 Infrastructure Cybersecurity, Version 1.1 (National Institute of Standards and Technology,
649 Gaithersburg, MD). <https://doi.org/10.6028/NIST.CSWP.6>
- 650 [2] Barrett MP, Keller N, Quinn SD, Smith MC, Scarfone KA (2022) National Online
651 Informative References (OLIR) Program: Submission Guidance for OLIR Developers.
652 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or
653 Internal Report (IR) 8278A. <https://doi.org/10.6028/NIST.IR.8278Ar1.ipd>
- 654 [3] National Institute of Standards and Technology (2020) The NIST Privacy Framework: A
655 Tool for Improving Privacy through Enterprise Risk Management, Version 1.0 (National
656 Institute of Standards and Technology, Gaithersburg, MD).
657 <https://doi.org/10.6028/NIST.CSWP.10>
- 658 [4] Fagan MJ, Megas KN, Scarfone KA, Smith M (2020) IoT Device Cybersecurity Capability
659 Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
660 Interagency or Internal Report (IR) 8259A. <https://doi.org/10.6028/NIST.IR.8259A>
- 661 [5] Joint Task Force Transformation Initiative (2020) Security and Privacy Controls for
662 Information Systems and Organizations. (National Institute of Standards and Technology,
663 Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of
664 December 10, 2020. <https://doi.org/10.6028/NIST.SP.800-53r5>
- 665 [6] Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled
666 Unclassified Information in Nonfederal Systems and Organizations. (National Institute of
667 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171,
668 Rev. 2. <https://doi.org/10.6028/NIST.SP.800-171r2>
669

670 **Appendix A. List of Symbols, Abbreviations, and Acronyms**

671 **CPRT**

672 Cybersecurity and Privacy Reference Tool

673 **CSV**

674 Comma-Separated Values

675 **DRM**

676 Derived Relationship Mapping

677 **FOIA**

678 Freedom of Information Act

679 **ICT**

680 Information and Communication Technology

681 **IoT**

682 Internet of Things

683 **IR**

684 Interagency or Internal Report

685 **ITL**

686 Information Technology Laboratory

687 **JSON**

688 JavaScript Object Notation

689 **NIST**

690 National Institute of Standards and Technology

691 **OLIR**

692 Online Informative References

693 **SME**

694 Subject Matter Expert

695 **SP**

696 Special Publication

697 **URL**

698 Uniform Resource Locator

699 **USG**

700 United States Government

701 **Appendix B. Glossary**

702 **crosswalk OLIR**

703 An OLIR that indicates relationships between pairs of elements without additional characterization of those
704 relationships.

705 **Derived Relationship Mapping**

706 A potential mapping between Reference Document Elements identified by finding elements from two or more
707 Reference Documents that map to the same Focal Document Element.

708 **Developer**

709 See *OLIR Developer*.

710 **Focal Document**

711 A source document that is used as the basis for comparing its elements with elements from another document.
712 Examples of Focal Documents include the Cybersecurity Framework version 1.1, the Privacy Framework version
713 1.0, and SP 800-53, Revision 5.

714 **Focal Document Element**

715 A discrete section, sentence, phrase, or other identifiable piece of content of a Focal Document.

716 **Informative Reference**

717 See *Online Informative Reference*.

718 **Informative Reference Developer**

719 See *OLIR Developer*.

720 **mapping OLIR**

721 An OLIR that characterizes each relationship between pairs of elements, including the rationale for indicating the
722 connection between the elements and the relationship type based on set theory principles.

723 **non-owner**

724 An OLIR produced by anyone other than the owner of the Reference Document.

725 **OLIR Catalog**

726 The National OLIR Program's online site for sharing OLIRs.

727 **OLIR Developer**

728 A person, team, or organization that creates an OLIR and submits it to the National OLIR Program.

729 **Online Informative Reference**

730 Relationships between elements of two documents that are recorded in a NIST IR 8278A-compliant format and
731 shared by the OLIR Catalog. There are two types of OLIRs: crosswalk and mapping.

732 **owner**

733 An OLIR produced by the owner of the Reference Document.

734 **Reference**

735 See *Online Informative Reference*.

736 **Reference Document**

737 A document being compared to a Focal Document, such as traditional documents, products, services, education
738 materials, and training.

739 **Reference Document Element**

740 A discrete section, sentence, phrase, or other identifiable piece of content of a Reference Document.

741 **Appendix C. Change Log**

742 In Revision 1 (NIST IR 8278r1), the following changes were made to this report:

- 743 • Reorganized the content and made editorial changes throughout the report to improve
744 clarity and usability
- 745 • Reformatted all content to follow the latest NIST technical report template
- 746 • Updated content throughout the report to reflect recent changes to OLIR, such as
747 eliminated the tiers concept for reference data and added the concept of unilateral and
748 bilateral OLIRs
- 749 • Section 2.3 – Created new subsection on the NIST Cybersecurity and Privacy Reference
750 Tool (CPRT)