

3 **Managing the Security**  
4 **of Information Exchanges**

---

5  
6  
7 Kelley Dempsey  
8 Victoria Pillitteri  
9 Andrew Regenscheid

10  
11  
12  
13  
14 This publication is available free of charge from:  
15 <https://doi.org/10.6028/NIST.SP.800-47r1-draft>  
16  
17  
18

19  
20  
  
21  
22  
23  
  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41

**Draft NIST Special Publication 800-47  
Revision 1**

**Managing the Security  
of Information Exchanges**

Kelley Dempsey  
Victoria Pillitteri  
Andrew Regenscheid  
*Computer Security Division  
Information Technology Laboratory*

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-47r1-draft>

January 2021



U.S. Department of Commerce  
*Wynn Coggins, Acting Secretary*

National Institute of Standards and Technology  
*James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce  
for Standards and Technology & Director, National Institute of Standards and Technology*

42  
43  
44  
45  
46  
47  
48  
49  
50

51

## Authority

52 This publication has been developed by NIST to further its statutory responsibilities under the Federal  
53 Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-  
54 283. NIST is responsible for developing information security standards and guidelines, including  
55 minimum requirements for federal information systems. Such information security standards and  
56 guidelines shall not apply to national security systems without the express approval of the appropriate  
57 federal officials exercising policy authority over such systems. This guideline is consistent with the  
58 requirements of the Office of Management and Budget (OMB) Circular A-130.

59 Nothing in this publication should be taken to contradict the standards and guidelines made mandatory  
60 and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should  
61 these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of  
62 Commerce, OMB Director, or any other federal official. This publication may be used by nongovernmental  
63 organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would,  
64 however, be appreciated by NIST.

65 National Institute of Standards and Technology Special Publication 800-47 Revision 1  
66 Natl. Inst. Stand. Technol. Spec. Publ. 800-47 Revision 1, 58 pages (January 2021)  
67 CODEN: NSPUE2  
68

69 This publication is available free of charge from:  
70 <https://doi.org/10.6028/NIST.SP.800-47r1-draft>

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

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

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

84

85 **Public comment period: *January 26, 2021 through March 12, 2021***

86 National Institute of Standards and Technology  
87 Attn: Computer Security Division, Information Technology Laboratory  
88 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930  
89 Email: [sec-cert@nist.gov](mailto:sec-cert@nist.gov)

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

## 91 **Reports on Computer Systems Technology**

92 The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology  
93 (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's  
94 measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of  
95 concept implementations, and technical analyses to advance the development and productive use of  
96 information technology. ITL's responsibilities include the development of management, administrative,  
97 technical, and physical standards and guidelines for the cost-effective security and privacy of other than  
98 national security-related information in federal information systems. The Special Publication 800-series  
99 reports on ITL's research, guidelines, and outreach efforts in information system security, and its  
100 collaborative activities with industry, government, and academic organizations.

### 101 **Abstract**

102 An organization often has mission and business-based needs to exchange (share) information with one  
103 or more other internal or external organizations via various information exchange channels; however, it  
104 is recognized that the information being exchanged also requires the same or similar level of protection  
105 as it moves from one organization to another (protection commensurate with risk).

106 This publication focuses managing the protection of the information being exchanged or accessed  
107 before, during, and after the exchange rather than on any particular type of technology-based  
108 connection or information access or exchange method and thus provides guidance on identifying  
109 information exchanges, considerations for protecting exchanged information, and the agreement(s)  
110 needed to help manage protection of the exchanged information. Organizations are expected to tailor  
111 the guidance to meet specific organizational needs and requirements regarding the information  
112 exchange.

### 113 **Keywords**

114 agreements; connection; information exchange; information exchange agreement; interconnection;  
115 interconnection security agreement; memoranda of agreement; memoranda of understanding;  
116 nondisclosure agreement; protection requirements; risk management; service level agreement; user  
117 agreement.

118

119

## Acknowledgments

120 The authors, Kelley Dempsey, Victoria Pillitteri, and Andrew Regenscheid wish to thank their colleagues  
121 who reviewed drafts of this publication and provided valuable input, including Joseph Boone, Joshua  
122 Finney, Stephen Ford, Greg Frassmann, Ann Galchutt, Jay Gazlay, Nedim Goren, Alan McClelland, Douglas  
123 Montgomery, Thomas Ritz, Scott Rose, John Simms, and Scott Spitnale. The authors also gratefully  
124 acknowledge the work of the original authors of SP 800-47, Tim Grance, Joan Hash, Steven Peck,  
125 Jonathan Smith, and Karen Korow-Diks, as well as the preliminary updates made by Michael Nieles.

126

127

128

## Note to Reviewers

129 In addition to updating terms and references for consistency with Special Publication (SP) 800-37  
130 Revision 2 and SP 800-53 Revision 5, SP 800-47 Revision 1 has been expanded to focus on managing the  
131 security of information being exchanged commensurate with risk as opposed to focusing on only  
132 managing the security of the specific method of exchange. An important outcome of managing the  
133 security of information exchanges is to select and document appropriate agreements to govern the  
134 information exchange between exchanging parties. Several types of agreements are addressed in SP  
135 800-47 Revision 1, and it is expected that more than one agreement type may be needed. A matrix is  
136 provided to help organizations determine which agreement types are needed.

137 NIST is interested in feedback on Draft SP 800-47, Revision 1, specifically on:

- 138 1. Whether the agreements addressed herein represent a comprehensive set of agreements that  
139 may be needed to manage the security of information being exchanged.
- 140 2. Whether the matrix provided will be helpful to organizations in determining appropriate  
141 agreement types. Please provide details on how and why it is or is not helpful in determining  
142 appropriate agreement types.
- 143 3. Are there additional types of agreements needed to manage the security of information being  
144 exchanged across authorization boundaries? Please provide examples of additional  
145 agreements, if feasible.
- 146 4. Are there additional resources that NIST can provide or develop to manage security of  
147 information exchanges?

148 As with SP 800-37 and SP 800-53, SP 800-47 is technology-neutral and is intended to be implementable  
149 for any type of organization and any type of information exchange.

150

151

152

## Call for Patent Claims

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

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

- 161 a) assurance in the form of a general disclaimer to the effect that such party does not hold and  
162 does not currently intend holding any essential patent claim(s); or
- 163 b) assurance that a license to such essential patent claim(s) will be made available to applicants  
164 desiring to utilize the license for the purpose of complying with the guidance or requirements in  
165 this ITL draft publication either:
- 166 i. under reasonable terms and conditions that are demonstrably free of any unfair  
167 discrimination; or
  - 168 ii. without compensation and under reasonable terms and conditions that are  
169 demonstrably free of any unfair discrimination.

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

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

177 Such statements should be addressed to: [sec-cert@nist.gov](mailto:sec-cert@nist.gov)

## 178 **Executive Summary**

179 Managing the Security of Information Exchanges provides guidance for planning, establishing,  
180 maintaining, and discontinuing information exchange and access between systems that are owned and  
181 operated by different organizations (internal or external) or that cross authorization boundaries. The  
182 guidance is consistent with the requirements specified in the Office of Management and Budget ([OMB](#))  
183 [Circular A-130](#) for the secure management of information exchanges.

184 This guidance defines the scope of information exchange, describes the benefits of the secure  
185 management of information exchange, identifies types of information exchanges, discusses potential  
186 security risks associated with information exchange, and discusses several types of agreements that may  
187 be applied by organizations with a mission or business need to exchange information.

188 An approach for securely managing information exchange between systems and organizations is  
189 presented. The following four phases of information exchange management are addressed:

- 190 1. **Planning the information exchange:** The participating organizations perform preliminary  
191 activities; examine all relevant technical, security, and administrative issues; and develop an  
192 appropriate agreement to govern the management and use of the information and how it is to  
193 be exchanged (e.g., via a dedicated circuit or virtual private network, database sharing, cloud- or  
194 web-based services, simple file exchange).
- 195 2. **Establishing the information exchange:** The organizations develop and execute a plan for  
196 establishing the information exchange, including implementing or configuring appropriate  
197 security controls and developing and signing appropriate agreements.
- 198 3. **Maintaining the exchange and associated agreements:** The organizations actively maintain the  
199 security of the information exchange after it is established and ensure that the terms of the  
200 associated agreements are met and remain relevant, including reviewing and renewing the  
201 agreements at an agreed-upon frequency.
- 202 4. **Discontinuing the information exchange:** Information exchange may be temporary, or at some  
203 point, the organizations may need to discontinue the information exchange. Whether the  
204 exchange was temporary or long-term, the conclusion of an information exchange is conducted  
205 in a manner that avoids disrupting any other party's system. In response to an incident or other  
206 emergency, however, the organizations may decide to discontinue the information exchange  
207 immediately.

208 This publication provides recommended steps for completing each phase with an emphasis on the  
209 security measures necessary to protect the shared data.

210 Also included is information for selecting and developing appropriate information exchange agreements  
211 and agreement templates. Agreements specify the responsibilities of participating organizations and the  
212 technical and security requirements for the information exchange.

213  
214

**Table of Contents**

215 **Executive Summary ..... v**

216 **1 Introduction ..... 1**

217     1.1 Purpose and Applicability ..... 1

218     1.2 Target Audience ..... 1

219     1.3 Organization of this Publication ..... 1

220 **2 The Fundamentals ..... 3**

221     2.1 Types of Information Exchange ..... 4

222         2.1.1 System Interconnections ..... 5

223         2.1.2 Information Exchanges ..... 7

224     2.2 Information Exchange: Accessing or Transferring the Information ..... 8

225 **3 Information Exchange Security Management ..... 9**

226     3.1. Planning an Information Exchange ..... 10

227         3.1.1 Step 1: Establish a Joint Planning Team ..... 11

228         3.1.2 Step 2: Define the Business Case ..... 12

229         3.1.3 Step 3: Apply the NIST Risk Management Framework ..... 12

230         3.1.4 Step 4: Identify Specific Protection Requirements ..... 12

231         3.1.5 Step 5: Document Appropriate Agreements ..... 17

232         3.1.6 Step 6: Approve or Reject the Information Exchange ..... 20

233     3.2 Establishing the Information Exchange ..... 22

234         3.2.1 Step 1: Develop an Implementation Plan ..... 22

235         3.2.2 Step 2: Execute the Implementation Plan ..... 23

236         3.2.3 Step 3: Activate the Information Exchange ..... 24

237     3.3 Maintaining the Information Exchange ..... 25

238         3.3.1 Maintain Clear Lines of Communication ..... 25

239         3.3.2 Maintain Systems and System Components ..... 26

240         3.3.3 Manage User Accounts ..... 26

241         3.3.4 Conduct Security Assessments ..... 26

242         3.3.5 Analyze Event Logs ..... 26

243         3.3.6 Report and Respond to Security Incidents ..... 27

244         3.3.7 Coordinate Contingency Planning Activities ..... 27

245         3.3.8 Manage Configuration Changes ..... 27



246 3.3.9 Review and Maintain System Security Plans and Applicable  
 247 Agreements ..... 28  
 248 3.3.10 Review the Continued Need for the Information Exchange ..... 28  
 249 3.4 Discontinuing the Information Exchange ..... 29  
 250 3.4.1 Planned Discontinuance ..... 29  
 251 3.4.2 Emergency Discontinuance ..... 30  
 252 3.4.3 Resumption of Interconnection ..... 30  
 253 **References ..... 32**

254  
 255 **List of Appendices**

256 **Appendix A— Glossary ..... 37**  
 257 **Appendix B— Acronyms and Abbreviations ..... 39**  
 258 **Appendix C— Agreement Templates and Guidance ..... 41**

259  
 260 **List of Figures**

261 Figure 1: System Interconnections ..... 7  
 262 Figure 2: Phases of Information Exchange Management ..... 10  
 263 Figure 3: Information Exchange Planning Phase ..... 11  
 264 Figure 4: Information Exchange Establish Phase ..... 22  
 265 Figure 5: Information Exchange Maintain Phase ..... 25  
 266 Figure 6: Information Exchange Discontinue Phase ..... 29

267  
 268 **List of Tables**

269 Table 1: Potential Agreements Matrix ..... 18  
 270

## 271 **1 Introduction**

272 An organization often has mission and business-based needs to share or exchange information with one  
273 or more other internal or external organizations via various information exchange methods; however, it  
274 is recognized that the information being exchanged also requires the same or similar level of protection  
275 as it moves from one organization to another (protection commensurate with risk).

276 This publication focuses on managing the protection of the information being exchanged or accessed  
277 before, during, and after the exchange in a manner commensurate with risk rather than on any  
278 particular type of technology-based connection or information access or exchange method and thus  
279 provides guidance on identifying information exchanges and the appropriate agreement(s) needed to  
280 help manage the protection of the exchanged information. Organizations are expected to tailor the  
281 guidance to meet specific organizational needs and requirements regarding the information exchange.

### 282 **1.1 Purpose and Applicability**

283 This publication provides guidance for managing (i.e., planning, establishing, maintaining, and  
284 discontinuing) the security of information exchanges between systems that are owned and operated by  
285 different organizations or are within the same organization but with different authorization boundaries,  
286 including organizations within a single federal agency. Organizations manage the security of the  
287 information being exchanged by applying security controls and entering into agreements designed to  
288 manage risk and protect the information being exchanged at the same or similar level.

289 This publication is published by the National Institute of Standards and Technology (NIST) as  
290 recommended guidance for federal agencies. It also may be used by nonfederal organizations.

291 Federal agencies rely on applicable laws, regulations, and policies for exchanging information between  
292 systems that are used to store, process, and disseminate classified data.

### 293 **1.2 Target Audience**

294 This publication is intended for the Senior Accountable Official for Risk Management/Risk Executive  
295 (function), authorizing officials, system owners, information owners, program managers, security  
296 officers, system architects, system administrators, and network administrators who are responsible for  
297 planning, approving, establishing, maintaining, or discontinuing information exchanges and access  
298 between systems. Specific information exchange technologies are not addressed (i.e., the guidance is  
299 technology-neutral and can be applied to any type of information exchange between any types of  
300 organizations).

### 301 **1.3 Organization of this Publication**

302 This publication is organized into three sections and four appendices. Section 1 introduces the  
303 document. [Section 2](#) discusses the document's purpose and benefits, as well as the types and methods  
304 of information exchanges. [Section 3](#) describes four phases for managing the security of information  
305 exchanges and provides a matrix to help organizations determine the types of agreements needed to  
306 manage the security of the information exchange.

307 A [References](#) section provides references information. [Appendix A](#) provides glossary information.  
308 [Appendix B](#) provides acronym and abbreviation translations. [Appendix C](#) provides examples of some  
309 agreement types.

## 310 2 The Fundamentals

311 Information exchange includes **access to or the transfer of data outside of authorization boundaries** in  
312 order to accomplish a mission or business function. When information is accessed or passed across the  
313 authorization boundary from one system to another system, one or more agreements are used to  
314 specify the responsibilities of each organization, the types and impact level of information to be  
315 accessed or exchanged, how the exchanged information is to be used, and how the information is to be  
316 protected when it is processed, stored, or transmitted on both ends of the exchange. The type of  
317 agreement(s) selected and the level of effort required to develop and maintain the agreement are based  
318 on factors including, but not limited to, the impact level of the information being exchanged, the  
319 relationship between the organizations exchanging information (e.g., internal organization to internal  
320 organization, government to government, government to business, business to business, government or  
321 business to service provider, government or business to individual), the resiliency requirements of the  
322 information exchange, and the level of access to the system and information by users of the other  
323 systems and organizations.

324 Organizations choose to exchange information for a variety of reasons, depending on organizational  
325 needs. For example, organizations may exchange information to:

- 326 • Share data and information among authorized users
- 327 • Provide customized levels of access to data
- 328 • Collaborate on joint projects
- 329 • Provide full, part-time, intermittent, permanent, or temporary communications
- 330 • Reduce data collection efforts
- 331 • Provide online training
- 332 • Provide secure storage for critical data and backup files

333 Significant benefits can be realized through information exchange, such as reduced operating costs,  
334 greater functionality, improved efficiency, centralized access to data, and reduction of duplicative  
335 datasets. Information exchange between systems may also strengthen ties among participating  
336 organizations by promoting communication and cooperation.

337 Despite the advantages, information exchange exposes the participating organizations to risk. If the  
338 information exchange is not properly planned and managed, a failure to protect the information from a  
339 loss of confidentiality, integrity, or availability could compromise the information and associated  
340 systems. Similarly, if one of the systems is compromised, the exchanged information could be  
341 compromised, or an interconnection used to exchange information could be leveraged as a conduit to  
342 compromise the other system and information. The risk is underscored because, in most cases, the  
343 participating organizations have little or no control over the operation and management of the other  
344 organization's system. Additionally, each participating organization may have differing risk tolerances  
345 associated with the information exchange and dependencies to facilitate and rely on the exchange.

346 Therefore, it is critical that the participating organizations learn as much as possible about the risks  
347 associated with the information exchange<sup>1</sup> and what security controls can be implemented to mitigate  
348 those risks. Depending on the type of information exchange and the impact level of the information  
349 being exchanged, it may also be critical that the organizations establish and formally document one or  
350 more agreements regarding the management and use of the exchanged information and the operation  
351 of any interconnection used to exchange the information. Senior managers from each organization are  
352 responsible for reviewing, approving, and signing the agreement (e.g., Risk Executive (function) [RE(f)],  
353 Chief Information Officer [CIO], Chief Information Security Officer [CISO], Authorizing Official [AO]).<sup>2</sup>

## 354 **2.1 Types of Information Exchange**

355 Information exchange occurs via communications technology usually provided by an internet service  
356 provider (ISP) or via a system interconnection (physical or virtual), which may itself employ the services  
357 of an ISP or telecommunications vendor. Methods to exchange information, and for which some type of  
358 information exchange agreement<sup>3</sup> may be warranted, include, but are not limited to, direct exchange  
359 (including access) across a system interconnection, electronic or digital file transfers, file-sharing  
360 services, database access/sharing or exchanges of database transaction information, exchange of  
361 information via portable storage device, and email exchange.

362 Excluded from information exchanges and information exchange agreements are public services (e.g.,  
363 time service), users accessing publicly available websites via a web browser, connections with an ISP,  
364 and organizational users logging into the organizational network via an organization-approved endpoint.  
365 Organizations and users accessing a publicly available service or website need not be included in the  
366 scope of this document, as public information may not need safeguards on protection, use, or further  
367 distribution. However, protected information distributed via a website may be in-scope if users are  
368 expected to abide by any terms and conditions prior to be given access to the information. Furthermore,  
369 the connection between an organization and an ISP is not used to exchange information between the  
370 organization and the ISP. Rather, the ISP connection provides a communications channel that allows the  
371 organization to exchange information with other organizations.

372 The types of information to be exchanged, the impact levels of the information being exchanged, and  
373 how the information is to be used by the other organization are agreed upon by participating  
374 organizations to manage risk and address information security requirements for information exchanges  
375 regardless of the particular method of exchange. Such knowledge facilitates the appropriate level of  
376 information protection needed for transmission and when the information is processed or stored at the  
377 other organization and helps organizations determine the types of agreements, if any, that are needed  
378 for the exchange. The organization considers agreement types such as interconnection security  
379 agreements, interconnection exchange agreements, non-disclosure agreements, access agreements,  
380 and/or acceptable use agreements, as described in [Section 3.1.5](#).

---

<sup>1</sup> A risk assessment includes the determination of threats, vulnerabilities, likelihoods, and impacts. See [\[SP 800-30\]](#) for additional information on conducting risk assessments.

<sup>2</sup> See [\[SP 800-37\]](#) for additional information on information security roles and responsibilities.

<sup>3</sup> [\[OMB Circular A-130\]](#) requires agreements (e.g., memoranda of understanding, interconnection security agreements, contracts) for interfaces between systems used or operated by contractors or other entities on behalf of the Federal Government or that collect or maintain federal information on behalf of the Federal Government and agency-owned or operated systems.

### 381 **2.1.1 System Interconnections**

382 A system interconnection is defined as a direct connection between two or more systems in different  
383 authorization boundaries for the purpose of exchanging information and/or allowing access to  
384 information, information services, and resources. An interconnection used for information exchange has  
385 at least three basic components: two (or more) endpoints and the mechanism by which the data flows  
386 (i.e., the “pipe” through which information is exchanged). The interconnection can be made from one  
387 location to another location or from one location to several locations. In this publication, it is assumed  
388 that the systems being interconnected are in different authorization boundaries, are owned and  
389 operated by different organizations, or are separately managed entities within the same organization.  
390 That is, management of the security of information exchanges is needed not only when information is  
391 exchanged between different organizations, but also when it is exchanged across authorization  
392 boundaries within a given organization.

393 A system interconnection is made via a dedicated or on-demand circuit (e.g., leased lines) or via a virtual  
394 connection using a Virtual Private Network (VPN)<sup>4</sup> solution (e.g., Internet Protocol Security [IPsec],  
395 Secure Sockets Layer Virtual Private Network [SSLVPN], Layer Two Tunneling Protocol [L2TP]).

396 The dedicated or on-demand circuit or the VPN is the “pipe” that connects the systems. Employment of  
397 a dedicated circuit may be more expensive, but it provides greater security assurance for the  
398 information exchange because the circuit may be breached only through a direct physical intrusion.

399 The less expensive alternative is to connect systems over a public network (e.g., the internet) using a  
400 VPN. A VPN is a network that enables two or more parties to communicate securely across a public  
401 network by creating a private connection, or “tunnel,” between endpoints. Information transmitted via  
402 VPN over a public network can be intercepted by unauthorized parties; however, the use of  
403 authentication and encryption helps ensure the confidentiality and integrity of the information  
404 exchange.

405 The decision to exchange information via a system interconnection is based on an assessment of the  
406 associated risks. [\[SP 800-30\]](#), *Guide for Conducting Risk Assessments*, provides guidance on conducting  
407 risk assessments and addresses the determination of threats, vulnerabilities, the likelihood of  
408 occurrence, and the impact of occurrence on the mission. Organizations participating in the information  
409 exchange conduct risk assessments to determine the risks of exchanging information and  
410 interconnecting systems from each organization’s perspective.

411 System interconnections can operate at a network level or an application level:

- 412 • Network Interconnection: A physical or virtual communications link between two or more  
413 networks operated by different organizations or operated within the same organization but  
414 within different authorization boundaries.
- 415 • Application Interconnection: A logical communications link between two or more  
416 applications operated by different organizations or within the same organization but within  
417 different authorization boundaries used to exchange information or provide information

---

<sup>4</sup> For information on implementing secure VPNs, see [\[SP 800-77\]](#), *Guide to IPsec VPNs*, and [\[SP 800-113\]](#), *Guide to SSL VPNs*.

418 services (e.g., authentication, logging). Application interconnections include file-sharing  
419 services or applications and information exchange feeds that occur at the session,  
420 presentation, or application layer.

421 System interconnections can include permanent connections or temporary connections established for a  
422 specific period of time (or function):

- 423 • Permanent (always on) Connection

424 A permanent connection is a perpetual communication channel. Permanent connections are  
425 most often made via a dedicated circuit.

- 426 • Scheduled Data Transfer

427 A scheduled data transfer is a connection used to transfer data on a regular, recurring basis.  
428 For example, every Friday evening, weekly payroll information is shared between an  
429 organization and that organization's payroll service provider. Scheduled data transfers may  
430 be via a dedicated circuit or virtual connection.

- 431 • Intermittent Ad-hoc Connection

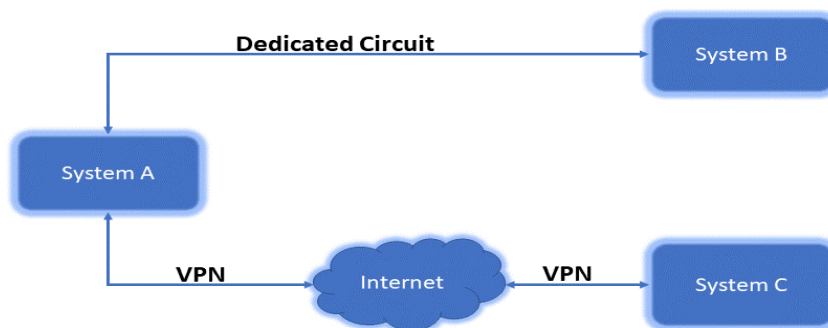
432 An intermittent, ad-hoc connection is a needs-based connection that is initiated for a  
433 specific time or purpose after which the connection is terminated. Intermittent connections  
434 are most often made via virtual connection.

435 To address information security requirements for system interconnections, an interconnection security  
436 agreement (ISA) that specifies the security requirements expected for the impact level of the  
437 information being exchanged for all participating systems is recommended. ISAs are often coupled with  
438 Memoranda of Understanding/Agreement (MOU/A).<sup>5</sup> Example ISA and MOU/A templates are provided  
439 in [Appendix C](#). Other types of agreements may also be required and applied (e.g., contracts, non-  
440 disclosure agreements [NDA], access agreements, acceptable use agreements). See [Section 3.1.5](#) for  
441 more information on agreements.

442 The diagram below ([Figure 1](#)) illustrates two ways in which systems can be interconnected, as described  
443 in this section. In the figure, System A is connected to System B via a dedicated circuit. System A is  
444 connected to System C via a VPN tunnel.

---

<sup>5</sup> [\[OMB Circular A-130\]](#) requires agreements (e.g., memoranda of understanding, interconnection security agreements, contracts) for interfaces between systems used or operated by contractors or other entities on behalf of the Federal Government or that collect or maintain federal information on behalf of the Federal Government and agency owned or operated systems.



445

446

**Figure 1: System Interconnections**

### 447 2.1.2 Information Exchanges

448 Information can be exchanged using various methods via a system interconnection, an ISP, or both.  
 449 Common methods of information exchange include, but are not limited to, electronic or digital file  
 450 transfers, information exchange via portable storage device, information exchange via email, database  
 451 sharing or exchanges of database transaction information, and web or cloud-based services.

- 452 • Electronic/Digital File Transfers – An electronic or digital file transfer is the transmission of a  
 453 file (information) between two systems via a file transfer (communications) protocol. File  
 454 transfer protocols include file transfer protocol secure (FTPS), Hypertext Transfer Protocol  
 455 Secure (HTTPS), and Secure Copy Protocol (SCP).
- 456 • Email – Organizations often share information via email as file attachments. Organizations  
 457 consider the impact levels and implemented security controls for participating  
 458 organizations' email infrastructure to determine if the measures implemented to protect  
 459 the information being exchanged are adequate (e.g., email infrastructure protected at a  
 460 moderate impact level is insufficient to protect high impact information).
- 461 • Portable Storage Device – In some cases, information may have to be exchanged using a  
 462 portable storage device, such as removable discs (e.g., DVDs) or USB/thumb drives.  
 463 Organizations consider the impact level of the information being transferred as well as the  
 464 impact level of the system into which the information is to be transferred to determine if  
 465 measures implemented to protect the information being exchanged are adequate (e.g.,  
 466 chain of custody of the portable storage device).
- 467 • Database sharing or exchanges of database transaction information, including access to  
 468 information by users from another organization. Organizations consider the viability of  
 469 providing access to information instead of transferring it to reduce the instance of  
 470 duplicative datasets and the risk of the loss of confidentiality and integrity of the  
 471 information.



- 472
- 473
- 474
- File sharing services – File sharing services include, but are not limited to, information sharing and access to information via web-based file sharing or storage, such as Drop Box, Google Drive, MS Teams, or MS One Drive.

## 475 **2.2 Information Exchange: Accessing or Transferring the Information**

476 Information may be exchanged by accessing or transferring the information using one or more more of  
477 the methods described in [Section 2.1](#).

478 When information is exchanged via transfer, the information is duplicated in additional physical  
479 locations. Information transfer may lead to duplicative datasets, outdated information, or an increased  
480 risk of unauthorized disclosure or modification. However, the transfer of information may be indicated  
481 to support the use of the same information in a different mission or business process, different software  
482 application, or when it is otherwise not feasible to exchange information via system access.  
483 Organizations are advised to limit or restrict exchanged information to only the specific data needed to  
484 support the stated mission/business case rather than transferring the entire dataset. Participating  
485 organizations consider the impact of a loss of the confidentiality and integrity of the information being  
486 transferred as well as the need to protect the information commensurate with the agreed-upon impact  
487 level, regardless of its physical location.

488 When information is exchanged via system access, the information itself is not transferred but rather is  
489 accessed by users from participating organizations. Exchanging information via system access reduces  
490 the instances of duplicative datasets and the risk of loss of confidentiality and integrity of the  
491 information. As with any form of system access, the extent to which a user may access information  
492 resources is dependent on the organizational mission and the adverse impact of loss of confidentiality,  
493 integrity, and availability of the information. Accordingly, organizations may establish a limited  
494 exchange, whereby users are restricted to a single application, file, or file location with specific policies  
495 in place to govern access (e.g., access limited to read-only). Other organizations may establish more  
496 flexible exchanges, enabling users to access multiple applications, files, or databases. Still other  
497 organizations may establish exchanges that permit full transparency and access to the system and  
498 information.

499

### 3 Information Exchange Security Management

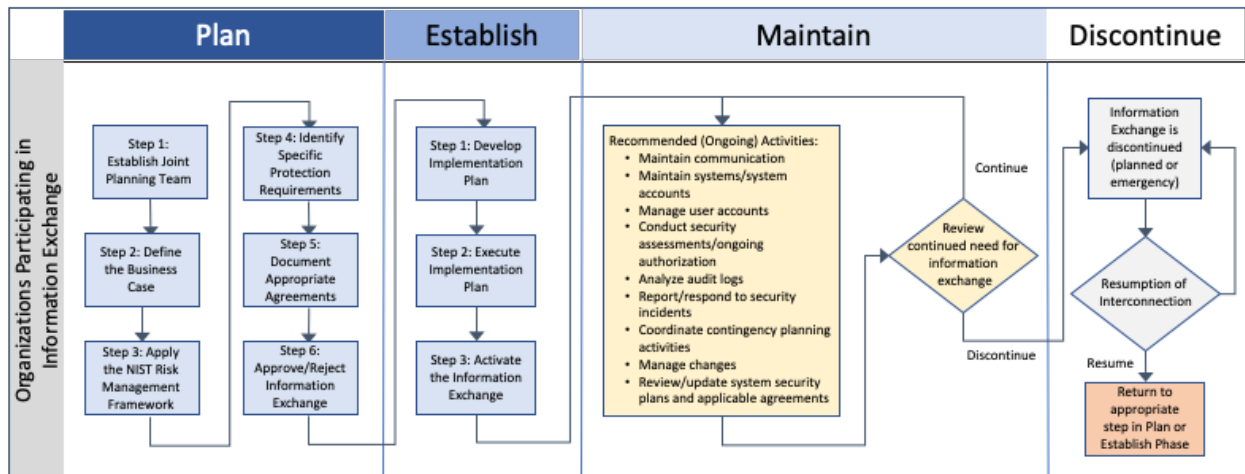
501 Risk-based management of information exchanges requires organizational-level governance to protect  
502 the information being exchanged with a level of effort that is commensurate with risk. Prior to any  
503 actual information exchange, the organization develops, documents, and disseminates policies and  
504 procedures governing information exchange. Decisions regarding the level of effort given to managing  
505 and protecting exchanged information—including the formality and rigor of planning, implementation,  
506 and the identification of formal agreement types needed—are based on organizational policy and  
507 procedures. Information exchange policies and procedures and decisions about how to manage and  
508 protect exchanged information are based on the impact of loss of the confidentiality, integrity, and  
509 availability of the information as determined by risk assessment and in accordance with organizational  
510 risk tolerance.

511 At a minimum, information exchange policy and procedures establish the types of information that can  
512 be shared without formal planning and agreements; the types of information that require tracking,  
513 formal planning, and agreements; and a process for determining the level of effort needed for  
514 exchanging types of information not specified in policy. For example, organizational policy might specify  
515 that exchanging low impact information via email does not require formal planning or a formal  
516 agreement, while exchanging moderate impact information via a file sharing service does require some  
517 formal planning and one or more formal agreements.

518 The remainder of this section describes four phases of information exchange management. Based on the  
519 level of effort needed to manage and protect exchanged information commensurate with risk and in  
520 accordance with organizational policies and procedures, organizations have the flexibility to determine  
521 the formality and rigor with which to apply the four phases and select the most appropriate agreements.

522 The four phases of information exchange management are described below and depicted in [Figure 2](#):

- 523 1. **Planning the information exchange:** The participating organizations conduct preliminary  
524 activities; examine all relevant technical, security, and administrative issues; and develop and  
525 sign appropriate agreements governing the management and use of the information and how it  
526 is to be exchanged (e.g., via an interconnection, file transfer, database sharing, web-based  
527 services, or a simple file exchange via email).
- 528 2. **Establishing the information exchange:** The organizations develop and execute a plan for  
529 establishing the information exchange, including implementing or configuring appropriate  
530 security controls and activating the exchange in accordance with organizational policies,  
531 procedures, and any signed agreements.
- 532 3. **Maintaining the exchange and associated agreements:** The organizations actively maintain the  
533 security of the information exchange after it is established and ensure that the terms of  
534 associated agreements are met and remain relevant.
- 535 4. **Discontinuing the information exchange:** At some point, the organizations may need to  
536 discontinue the information exchange. The conclusion of an information exchange is conducted  
537 in a manner that avoids disrupting organizational systems. In response to an incident or other  
538 emergency, however, the organizations may decide to discontinue the information exchange  
539 immediately.



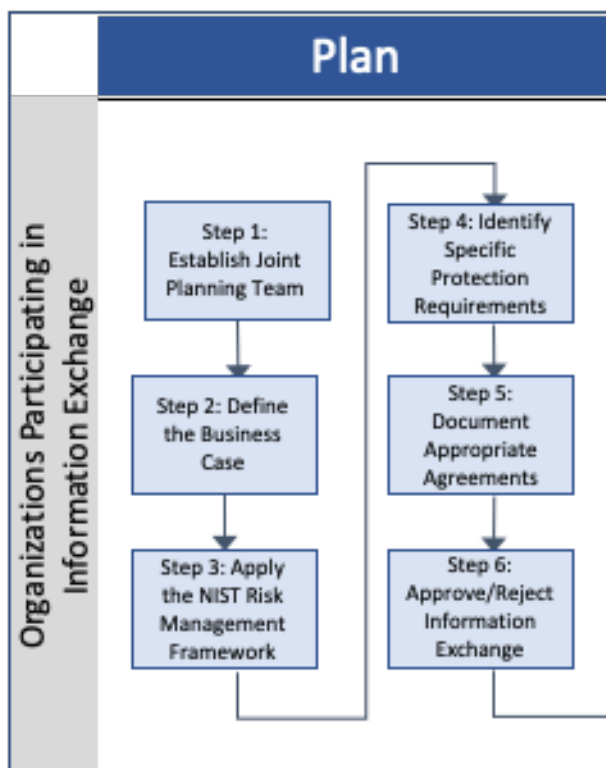
540

541

Figure 2: Phases of Information Exchange Management

542 **3.1. Planning an Information Exchange**

543 The process of exchanging information between two or more systems begins with a planning phase, in  
 544 which the participating organizations perform preliminary activities and examine the relevant technical,  
 545 security, and administrative issues, as shown in Figure 3. The purpose of the planning phase is to ensure  
 546 that the information exchange operates as efficiently and securely as possible. This section discusses  
 547 recommended steps for planning a system information exchange. The formality, structure, and rigor of  
 548 the planning phase steps depend on the type of exchange, the impact level of the information to be  
 549 exchanged, the relationship of the organizations involved in the exchange, and organizational policies  
 550 and procedures for information exchange.



551

552

Figure 3: Information Exchange Planning Phase

### 553 3.1.1 Step 1: Establish a Joint Planning Team

554 Each organization is responsible for ensuring the security of its respective systems and information and  
 555 for applying a well-coordinated approach to the information exchange, including regular  
 556 communications between the organizations throughout the phases of the exchange. Therefore, the  
 557 organizations consider establishing a joint planning team composed of representatives from  
 558 participating organizations that may include appropriate managerial and technical staff, mission and  
 559 business owners, system owners, information owners, system security officers, system administrators,  
 560 network administrators, and system security architects. The joint planning team could be part of an  
 561 existing working group or be created specifically for the planned information exchange. Regardless of  
 562 how it is formed, the commitment and support of the system and information owners and other senior  
 563 managers are important. The team is responsible for coordinating all aspects of the planning process  
 564 and ensuring that the process has clear direction, well-defined responsibilities, and sufficient resources.  
 565 The planning team may also remain active beyond the planning phase to serve as a forum for future  
 566 discussions about issues involving the information exchange.

567 In addition, members of the planning team coordinate with colleagues responsible for information  
 568 technology (IT) capital planning, configuration management, and other activities that may be associated  
 569 with the information exchange or related technology. In many cases, the information exchange is in part  
 570 or in whole a component of each organization's network. By coordinating the planning of the  
 571 information exchange with associated stakeholders, the organizations can reduce security risk, reduce  
 572 redundancy, and promote efficiency.

### 573 **3.1.2 Step 2: Define the Business Case**

574 The organizations work together to define the purpose of the information exchange, determine how the  
575 information exchange will support mission and business requirements, and identify potential costs and  
576 risks. Defining the business case establishes the basis of the information exchange and facilitates the  
577 planning process. Factors to consider are likely costs (e.g., staffing, equipment, and facilities), expected  
578 benefits (e.g., improved efficiency, centralized access to data), and potential risks (e.g., security,  
579 technical, privacy, legal, financial, etc.).

580 Note that there may be privacy statutes, regulations, or policies that place restrictions on the data to be  
581 exchanged. Examples of data that might be restricted include personally identifiable information such as  
582 names and social security numbers, or confidential business information such as contractor bid rates  
583 and trade secrets. Each organization consults with its Privacy Officer and/or Legal Counsel to determine  
584 whether the information to be exchanged may be shared, transferred, or accessed with the other  
585 organizations participating in the information exchange.

### 586 **3.1.3 Step 3: Apply the NIST Risk Management Framework**

587 Before exchanging information, each organization ensures that it has applied the Risk Management  
588 Framework (RMF) process to affected systems, as described in [\[SP 800-37\]](#), *Risk Management*  
589 *Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and*  
590 *Privacy*.

### 591 **3.1.4 Step 4: Identify Specific Protection Requirements**

592 The joint planning team identifies and examines relevant technical, security, and administrative issues  
593 surrounding the proposed information exchange. The results are used to develop the appropriate  
594 agreements needed to support and manage the information exchange and protect the information. The  
595 results may also be used to develop an implementation plan for establishing the information exchange.  
596 Note that changes made to existing systems in support of the information exchange, especially changes  
597 involving the addition of system components (i.e., hardware, software, or firmware) or changes to  
598 infrastructure, may necessitate revisiting one or more steps and tasks from the RMF.

599 The joint planning team considers the following issues:

- 600 • *Risk Assessment*: Participants in the information exchange may conduct a risk assessment to  
601 determine the impacts of a loss of confidentiality, integrity, and availability of the data to be  
602 exchanged to help ensure the appropriate level of protection and the availability of  
603 resources needed. The originating organization stipulates the protection requirements for  
604 the information in the agreements. If a risk assessment has already been conducted, the  
605 planning team considers the existing results and may need to update the results.
- 606 • *Information Security Risk Considerations*:
  - 607 – Minimize the data exchanged to reduce the risk of a loss of confidentiality and integrity
  - 608 outside of the authorization boundary.

- 609 – Consider increased risk if data that has been designated as a High Value Asset (HVA)<sup>6</sup> is to  
610 be exchanged.
- 611 – Consider the availability and resiliency requirements for the information exchange (also  
612 see *Dependencies* below).
- 613 – Consider whether the interconnections that participating organizations’ systems have with  
614 other systems and organizations could increase the risk of loss of confidentiality, integrity,  
615 and availability of exchanged information and organizational systems.
- 616 • *Impact Level*: Identify the impact of a loss of the information to be exchanged with respect  
617 to each of the three security objectives individually (i.e., confidentiality, integrity, and  
618 availability). Decisions about whether and how to share information may be different if the  
619 impact of a loss of availability is high but the impact of a loss of confidentiality is low versus  
620 the impact of a loss being moderate for integrity and low for availability. Identifying and  
621 agreeing to the information impact level is critical for determining the protection  
622 requirements for the exchanged information. See [\[SP 800-60\]](#), *Guide for Mapping Types of*  
623 *Information and Information Systems to Security Categories*; [\[FIPS 199\]](#), *Standards for*  
624 *Security Categorization of Federal Information and Information Systems*; and the Controlled  
625 Unclassified Information [\[\(CUI\) Registry\]](#) managed by the National Archives and Records  
626 Administration (NARA) for further guidance on identifying impact levels. Also see [\[SP 800-](#)  
627 [53\]](#) control RA-2.
- 628 • *Method of the information exchange*: Define the method of information exchange which  
629 may range from the adhoc emailing of files (limited data exchange) to a full system  
630 interconnection (exchange of information across a dedicated circuit or VPN).
- 631 • *Impact on Existing Infrastructure and Operations*: Determine whether the network  
632 infrastructure and system architecture currently used by participating organizations are  
633 sufficient to support the information exchange or whether additional infrastructure  
634 components are required (e.g., communication lines, routers, switches). If additional  
635 components are required, determine the potential impact that installing and using the  
636 components might have on the existing infrastructure, if any. In addition, determine the  
637 potential impacts that the information exchange could have on current operations (e.g.,  
638 increases in data traffic, new training requirements, and additional demands on system  
639 administration, security, and maintenance).
- 640 • *Dependencies*: Determine if one or more of the systems participating in the information  
641 exchange is dependent on the information to be exchanged or on the system  
642 interconnection itself for continued operation. If such dependencies exist, [\[SP 800-53\]](#)  
643 controls that support the availability objective for the system or information may warrant  
644 special attention (e.g., contingency planning, system or interconnection redundancies, or  
645 other resilience needs).
- 646 • *Specific Hardware Requirements*: Identify the hardware needed to support the information  
647 exchange (e.g., routers, firewalls, switches, servers, or workstations). Determine whether  
648 existing hardware is sufficient or whether additional components are required, especially if

---

<sup>6</sup> DHS published a Binding Operational Directive [\[DHS BOD 18-02\]](#) on Securing HVAs. DHS CISA provides a [\[HVA Control Overlay\]](#) and information on protecting HVAs.

- 649 future growth is anticipated. If new hardware is required, select products that are  
650 interoperable with existing hardware.
- 651 • *Specific Software Requirements*: Identify software needed to support the information  
652 exchange, including software for information exchange management and file sharing  
653 services, and on what hardware the software is to be installed (e.g., firewalls, servers,  
654 workstations, laptops). Determine whether existing software is sufficient, or whether  
655 additional software is required. If new software is required, select products that are  
656 interoperable with existing software.
  - 657 • *User Community*: Define the community of users requiring access to the exchanged  
658 information. Determine whether users are required to have specific employment status or  
659 nationality requirements as well as what level of background checks and/or security  
660 clearances are required. Devise an approach for compiling and managing the profiles of  
661 users requiring access to the exchanged information, including user identification and any  
662 other relevant information. Participating organizations use the user information to develop  
663 and maintain an approved access list or database of users with access to the exchanged  
664 information. Also see [\[SP 800-53\]](#) controls AC-2, Account Management; AC-3, Access  
665 Enforcement; IA-2, Identification and Authentication (Organizational Users); and IA-8,  
666 Identification and Authentication (Non-Organizational Users).
  - 667 • *Services and Applications*: Identify any information services to be provided by each  
668 organization as part of the information exchange as well as the applications associated with  
669 those services, if appropriate. Examples of services may include e-mail, secure file sharing  
670 services, authentication services, and general computational services.
  - 671 • *Roles and Responsibilities*: Identify the personnel responsible for establishing, maintaining,  
672 or managing the information exchange and specific responsibilities with respect to the  
673 information exchange. Affected personnel may include program managers, system owners,  
674 information owners, system and/or database administrators, and system security officers.  
675 Choose personnel who have appropriate subject matter expertise. Specific information on  
676 information security roles and responsibilities is available in [\[SP 800-37\]](#).
  - 677 • *Scheduling*: Develop a schedule for activities involved in planning, establishing, and  
678 maintaining the information exchange. Also, determine the schedule and conditions for  
679 terminating or reauthorizing the exchange. For example, all parties might agree to annually  
680 review agreements associated with the exchange to determine if the exchange is still  
681 needed and that the protection requirements remain sufficient.
  - 682 • *Costs and Budgeting*: Identify the expected costs required to plan, establish, and maintain  
683 the interconnection. Identify all associated costs, including labor, hardware, software,  
684 communications lines, applications, facilities, physical security, training, and testing. Also,  
685 identify costs for authorizing the information exchange after it is established, if appropriate.  
686 Develop a comprehensive budget, and determine how costs will be apportioned between  
687 the parties, if required.
  - 688 • *Data Element Naming*: If the information exchange involves databases, determine whether  
689 the data element naming schemes used by participating organizations are compatible or  
690 whether it is necessary to normalize databases so that the organizations can use the  
691 exchanged information. In addition, determine how to identify and resolve potential data  
692 element naming conflicts.



- 693
- 694
- 695
- 696
- 697
- 698
- *Information Ownership*: Determine whether ownership of exchanged information is transferred from the transmitting organization to the receiving organization or whether the transmitting organization retains ownership and the receiver is a custodian. As part of this effort, determine how exchanged information is stored, whether the information may be re-used or transferred to a third organization or system, and how information is destroyed when no longer needed.
  - *Security Controls*: Identify protection requirements to be implemented as controls to protect the confidentiality, integrity, and availability of the exchanged information and the systems processing, storing, or transmitting the information. Protection requirements are based on the impact of the potential loss of the confidentiality, integrity, or availability of the information and associated systems, organizational risk tolerance, and risk assessment results. If appropriate, organizations may begin with the relevant baseline set of controls, as identified in [\[SP 800-53B\]](#). Note that many of the issues addressed in this section (Section 3.1.4) are resolved by implementing controls in the baseline control sets but are included in this section to provide specifics on implementation for information exchange. Relevant [\[SP 800-53\]](#) controls are specified as appropriate.
    - *Separation of Duties*: Determine how the management or execution of duties associated with the information exchange is to be divided between the participating organizations and between the users of the information to be exchanged. Examples of duties that might be separated include auditing, managing user profiles, managing configurations, and maintaining equipment. Separation of duties reduces the risk that a single individual could cause harm to the exchanged information and the systems processing, storing, or transmitting the information, either accidentally or deliberately. See control AC-5, *Separation of Duties*, in [\[SP 800-53\]](#).
    - *Incident Reporting and Response*: Establish procedures to report and respond to anomalous and suspicious activity or actual incidents related to the information exchange that are detected by technology or staff in participating organizations. Incident reporting procedures are consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Determine when and how to notify each other about suspicious activity or security incidents that could affect the information exchange. Identify the types of incidents that require a report and the information to be included in the report, such as the cause of the incident, affected information or applications, and actual or potential impact. In addition, identify the types of incidents that require a coordinated response, and determine how to coordinate response activities. It might be appropriate to develop a joint incident response plan for this purpose. For more information, reference the Incident Response (IR) family of controls in [\[SP 800-53\]](#). SPs [\[800-61\]](#), [\[800-83\]](#), and [\[800-86\]](#) provide detailed information on incident response. Also see [\[US-Cert Federal Incident Notification Guidelines\]](#).
    - *Contingency Planning*: It may be necessary to have a contingency plan to respond to and recover from disasters or disruptive contingencies that could affect the information exchange, especially if the information exchange is moderate or high impact for availability. Organizations determine how to notify each other of such contingencies, the extent to which the organizations will assist each other, and the terms under which assistance will be provided. Identify emergency points of contact (POC). Determine whether to incorporate redundancy into components that support the information exchange, including redundant interconnection points, and how to retrieve backed up
- 709
- 710
- 711
- 712
- 713
- 714
- 715
- 716
- 717
- 718
- 719
- 720
- 721
- 722
- 723
- 724
- 725
- 726
- 727
- 728
- 729
- 730
- 731
- 732
- 733
- 734
- 735
- 736
- 737
- 738



- 739 information. Coordinate disaster response training, testing, and exercises. Additional  
740 information on the Contingency Planning (CP) family of controls can be found in [\[SP 800-  
741 53\]](#). [\[SP 800-34\]](#) provides detailed information on developing contingency plans.
- 742 – *Data Backup*: Determine backup and storage requirements for exchanged information. If  
743 backups are required, identify the types of information that require backup, the frequency  
744 of backups (e.g., daily, weekly, monthly), and which organization is responsible for the  
745 backups. Also, determine how to perform backups and how to link backups to contingency  
746 plan procedures. See controls in the Contingency Planning (CP) family (e.g., CP-6,  
747 *Alternate Site Storage*, and CP-9, *Information System Backup*) in [\[SP 800-53\]](#) for more  
748 specific guidance.
- 749 – *Configuration Management*: Determine how to coordinate the planning, design, and  
750 implementation of changes to the configuration baseline that could affect the security and  
751 functionality of the information exchange, such as upgrading hardware or software,  
752 changing configuration settings, or adding services. Establish a forum with relevant staff  
753 from each organization to review the proposed changes that may affect the information  
754 exchange. Coordinating configuration management activities reduces the potential for  
755 implementing changes that could introduce vulnerabilities or otherwise impact the  
756 confidentiality, integrity, or availability of the exchanged information or the systems  
757 processing, storing, or transmitting the information. Information on the Configuration  
758 Management (CM) family of controls is available in [\[SP 800-53\]](#). [\[SP 800-128\]](#), *Guide for  
759 Security-Focused Configuration Management of Information Systems*, provides detailed  
760 information on configuration management.
- 761 – *Rules of Behavior*: Develop rules of behavior that clearly delineate the responsibilities and  
762 expected behavior of personnel authorized to access the exchanged information and the  
763 systems processing, storing, or transmitting the information. Document the rules in  
764 writing, and state the consequences of inconsistent behavior or noncompliance. Cover the  
765 documented rules of behavior in a security training and awareness program. See control  
766 PL-4, *Rules of Behavior*, in [\[SP 800-53\]](#).
- 767 – *Training and Awareness*: Define training and awareness requirements for personnel  
768 authorized to access the exchanged information and the systems processing, storing, or  
769 transmitting the information. The information exchange training and awareness  
770 requirements may be incorporated into existing training and awareness activities. Training  
771 and awareness requirements may include the frequency and scheduling of training and  
772 the assignment of responsibility for conducting training and awareness activities. Design  
773 training to ensure that personnel are familiar with the relevant policies, procedures, and  
774 rules of behavior associated with the exchanged information and the systems that  
775 process, store, or transmit the information. Require users to sign an acknowledgement  
776 form indicating an understanding of security responsibilities with regard to the  
777 information exchange, if appropriate. If shared applications are used, ensure that users  
778 know how to use them properly. Additional information on the Awareness and Training  
779 (AT) family of controls is available in [\[SP 800-53\]](#). [\[SP 800-50\]](#) provides detailed  
780 information on building an information security awareness and training program. [\[SP 800-  
781 181\]](#) provides detailed information on a cybersecurity workforce framework. Additional  
782 information on information security education is available at the NIST [National Initiative  
783 for Cybersecurity Education \(NICE\)](#) website.

### 784 **3.1.5 Step 5: Document Appropriate Agreements<sup>7</sup>**

785 The joint planning team determines and documents the agreements needed to govern the exchanged  
786 information; the systems processing, storing, or transmitting the information; the roles and  
787 responsibilities of the affected organizations and users; the terms under which the organizations will  
788 abide by the agreement based on the team's review of relevant technical, security, and administrative  
789 issues (as described in [Section 3.1.4](#)); and other appropriate requirements. More than one type of  
790 agreement may be needed, such as an interconnection security agreement coupled with a non-  
791 disclosure agreement.

792 The Potential Agreements Matrix ([Table 1](#)) reflects agreements that may be needed based on the type  
793 or method of information exchange (rows) and the impact of a loss of that information (columns). The  
794 matrix is not intended to be prescriptive or limit the risk-based agreement choices by organizations but  
795 rather provides **initial** guidance to assist organizations in determining the most appropriate agreements.  
796 Additional criteria may also impact the types of agreements needed, including relevant technical,  
797 security, and administrative issues, as described in [Section 3.1.4](#).

798

799

---

<sup>7</sup> [\[OMB Circular A-130\]](#) requires agreements (e.g., memoranda of understanding, interconnection security agreements, contracts) for interfaces between the systems used or operated by contractors or other entities on behalf of the Federal Government or that collect or maintain federal information on behalf of the Federal Government and agency owned or operated systems.

800

**Table 1: Potential Agreements Matrix**

	<i>Low Impact Information</i>	<i>Moderate Impact Information</i>	<i>High Impact Information</i>
<b><i>Exchange via e-mail, portable media, or file transfer</i></b>	<i>Logged in tracking system</i>	<i>Logged in tracking system; Access Agreement; Acceptable Use Agreement; Non-disclosure Agreement</i>	<i>IEA; MOU/MOA; Access Agreement; Acceptable Use Agreement; Non-disclosure Agreement</i>
<b><i>Exchange via database- or web-based services</i></b>	<i>Logged in tracking system; contract</i>	<i>IEA; MOU/MOA; Access Agreement; Acceptable Use Agreement; Non-disclosure Agreement; contract</i>	<i>IEA; MOU/MOA; Access Agreement; Acceptable Use Agreement; Non-disclosure agreement; contract; service-level agreement</i>
<b><i>Exchange via system interconnection</i></b>	<i>ISA/MOU/MOA; contract</i>	<i>ISA/MOU/MOA; Access Agreement; Acceptable Use Agreement; Non-disclosure Agreement; contract; service-level agreement</i>	<i>ISA/MOU/MOA; Access agreement; Acceptable Use Agreement; Non-disclosure agreement; contract; service-level agreement</i>

801 Because the agreements themselves may contain information that is moderate impact or higher,  
 802 agreements are stored in accordance with impact level to protect against theft, damage, or destruction.  
 803 Examples of some agreement templates are provided in [Appendix C](#).

804 **3.1.5.1 Interconnection Security Agreement**

805 An interconnection security agreement (ISA) is a document that specifies the technical and security  
 806 requirements for establishing, operating, and maintaining an interconnection between two or more  
 807 systems. The ISA also supports a Memoranda of Understanding/Agreement (MOU/A) between the  
 808 organizations. Specifically, the ISA documents the requirements for connecting the systems; describes  
 809 the protection requirements and controls necessary to protect exchanged information and the systems  
 810 processing, storing, or transmitting the information; usually includes a topological drawing of the  
 811 interconnection; and provides a signature line for participating organizations. An ISA is indicated when  
 812 the information exchange occurs via an interconnection, as described in [Section 2.1.1](#). Note that the  
 813 organization may already have an interconnection and corresponding ISA with another organization  
 814 over which information exchanges occur between multiple systems and in support of multiple mission  
 815 requirements. In such situations, the information owner determines if the security protections and

816 processes specified in the existing ISA reduce risk to a level acceptable for the information to be  
817 exchanged. If the protections and processes are acceptable, additional agreements may still be required  
818 [\(see Table 1\)](#). If not, the ISA may be modified or a separate interconnection may be needed. An ISA  
819 template is provided in [Appendix C](#).

### 820 **3.1.5.2 Memoranda of Understanding (MOU) and/or Agreement (MOA)**

821 The MOU/A are often applied to information exchanges in conjunction with an ISA. In general, an MOU  
822 is a statement of intent between the participating organizations to work together and often states goals,  
823 objectives, or the purpose for the partnership; details the terms of and conditions for the agreement;  
824 and outlines the operations needed to achieve the goals or purpose. The MOA is most often used to  
825 address the financial responsibilities and obligations between the parties. While the MOA does not  
826 obligate funds, it could specify the authorities who can obligate funds. In support of information  
827 exchange, the MOU and MOA collectively address:

- 828 • Objectives and purpose for the information exchange;
- 829 • Relevant authorities and responsibilities of each organization;
- 830 • Terms and conditions for the agreement and exchanging information in a secure manner,  
831 including what constitutes acceptable use of the information to be exchanged;
- 832 • Financial responsibilities for the exchange; and
- 833 • Timeline for discontinuing or reauthorizing the information exchange.

834 The MOU and MOA do not include technical details on how the information exchange is established or  
835 maintained or specific security requirements for the exchange; that is the function of the ISA. An MOU/A  
836 is indicated for use in conjunction with an ISA when the information is exchanged via a system  
837 interconnection, as described in [Section 2.1.1](#), and may be indicated when moderate or high impact  
838 information is exchanged via database or web-based service or when high impact information is  
839 exchanged via email, portable storage device, or file transfer. Note that if there are no financial  
840 responsibilities associated with the exchange, the MOA may not be indicated. An MOU/A template and  
841 development guidance is provided in [Appendix C](#).

### 842 **3.1.5.3 Information Exchange Agreement**

843 An information exchange agreement (IEA) is a document that specifies protection requirements and  
844 responsibilities for information being exchanged. The IEA is similar to the ISA but does not include  
845 technical details associated with an interconnection. Specifically, the IEA describes the protection  
846 requirements and controls necessary to protect exchanged information and the systems processing,  
847 storing, or transmitting the information and provides a signature line for participating organizations. An  
848 IEA may be indicated when the information exchange occurs via one of the exchange methods described  
849 in [Section 2.1.2](#). An IEA template is provided in [Appendix C](#).

### 850 **3.1.5.4 Service-Level Agreement**

851 A service-level agreement (SLA) represents a commitment between a service provider and one or more  
852 customers and addresses specific aspects of the service, such as responsibilities, details on the type of  
853 service, expected performance level (e.g., reliability, acceptable quality, and response times), and  
854 requirements for reporting, resolution, and termination. Specific to information exchange and  
855 interconnections, SLAs explicitly address expectations regarding the **availability** of the connection used

856 to exchange the information. SLAs are often part of a formal contract. An SLA may be indicated for  
857 information exchange when the impact of a loss of availability is moderate or high and the information  
858 is exchanged via an interconnection provided as part of a contract with a service provider. [\[SP 800-35\]](#)  
859 provides information on information technology services and service-level agreements.

### 860 **3.1.5.5 User Agreement, Access Agreement, and Acceptable Use Agreement**

861 User agreements, access agreements, and acceptable use agreements are user-based agreements that  
862 are similar to rules of behavior and specify user responsibilities when exchanging information or  
863 accessing information or systems that contain the exchanged information. User responsibilities  
864 addressed in the agreement may include, but are not limited to, what the user is permitted to do with  
865 the information, how the information is to be used, and whether the information can be transmitted to  
866 other parties. Users with access to the information read and sign the agreement to acknowledge  
867 acceptance and understanding prior to being given access to the information. The user, access, or  
868 acceptable use agreement may be specific to the information being exchanged, or the participating  
869 organizations may determine that existing agreements or rules of behavior already read and signed by  
870 participating organizational users provide sufficient protection.

871 A user, access, or acceptable use agreement may be indicated for any type of information exchange  
872 when the information being exchanged is moderate or high impact.

### 873 **3.1.5.6 Non-disclosure Agreement**

874 A non-disclosure agreement (NDA) delineates specific information, materials, or knowledge that the  
875 signatories agree not to release or divulge to any other parties. An NDA may be valid for a defined time  
876 frame or may be indefinite.

877 A non-disclosure agreement may be indicated for information exchange when the information being  
878 exchanged is high impact for confidentiality or is personally identifiable information.

### 879 **3.1.5.7 Other Types of Agreements, Organization-Defined Agreement**

880 Contracts, agreements that combine elements of the other agreement types, internet service  
881 agreements, or other organization-defined agreements may also be applied to the information exchange  
882 as appropriate.

### 883 **3.1.5.8 Logged in Tracking System**

884 A tracking system provides a method to log and track information exchange outside of the authorization  
885 boundary. Examples of tracking systems include, but are not limited to, internal spreadsheets or  
886 databases; Governance, Risk and Compliance (GRC) tools or other automated tools; and keeping up-to-  
887 date control implementation information in a system security plan. Note that requirements for tracking  
888 information exchanges may be addressed as part of other types of agreements (e.g., ISA, IEA).

## 889 **3.1.6 Step 6: Approve or Reject the Information Exchange**

890 The joint planning team submits the proposed agreements to the relevant AO or other risk management  
891 official from each organization and requests approval for the information exchange. Upon receipt, the  
892 AOs or risk management officials review the proposed agreements as well as any other relevant  
893 documentation or activities. Based on the review, the AOs or risk management officials decide on one of  
894 the following:

- 895           • Approve the information exchange, or  
896           • Reject the information exchange.

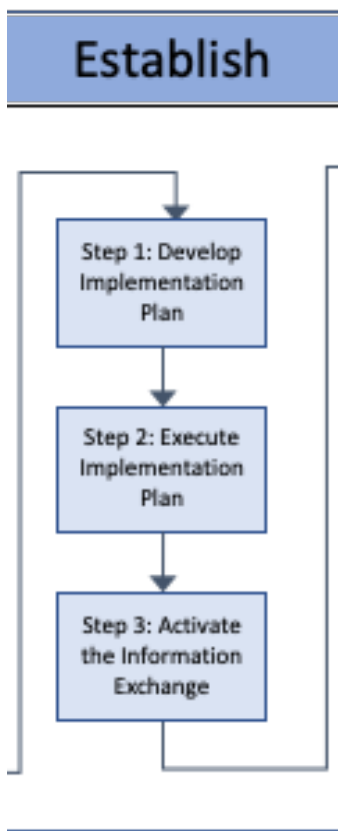
897 If the AOs or risk management officials accept the agreement(s), they sign and date the documents,  
898 thereby approving the information exchange. The agreements are then retained by participating  
899 organizations in accordance with organizational retention policies and procedures. Notify the  
900 appropriate program manager or any other officials responsible for the information and information  
901 exchange within each organization that the agreement to exchange information has been approved.

902 If the agreements are rejected by one or more AO or risk management official, the AO or risk  
903 management official may propose solutions and/or specify additional requirements to be completed  
904 before approval is granted, including the implementation of additional security controls. In addition, a  
905 timeline for completing the tasks is specified. The joint planning team works to meet the requirements,  
906 then resubmits the updated exchange agreements.

907

## 908 3.2 Establishing the Information Exchange

909 After the information exchange is planned and approved, it may be implemented. This section provides  
 910 recommended steps for establishing the information exchange, as shown in [Figure 4](#).



911

912

Figure 4: Information Exchange Establish Phase

### 913 3.2.1 Step 1: Develop an Implementation Plan

914 To ensure that information is exchanged securely, the joint planning team develops an information  
 915 exchange implementation plan. The purpose of the implementation plan is to centralize all aspects of  
 916 the information exchange effort in one document and to clarify how the technical requirements  
 917 specified in the agreement(s) will be implemented. A well-developed implementation plan greatly  
 918 improves the likelihood that the information exchange is implemented successfully and securely.

919 As appropriate, the implementation plan:

- 920 • Describes the systems involved in the information exchange
- 921 • Identifies the impact level of the information to be exchanged
- 922 • Identifies personnel responsible for establishing and maintaining the information exchange  
 923 and specifies their responsibilities
- 924 • Identifies implementation tasks and procedures
- 925 • Identifies and describes security controls implemented to protect the confidentiality,  
 926 integrity, and availability of the exchanged information
- 927 • Provides control assessment and measurement criteria to help ensure that the information

- 928 is exchanged securely
- 929 • Specifies training requirements for users (if applicable), including a training schedule
- 930 • Cites or includes all relevant documentation, such as system security plans, design
- 931 specifications, and standard operating procedures

### 932 **3.2.2 Step 2: Execute the Implementation Plan**

933 After the implementation plan is developed, reviewed, and approved by senior members of the planning

934 team, the plan may then be executed. A list of recommended tasks for implementing an information

935 exchange is provided below.

#### 936 **3.2.2.1 Install or Configure Hardware and Software**

937 It may be necessary to install new hardware and software or to configure existing hardware and

938 software to support the information exchange.

#### 940 **3.2.2.2 Implement or Configure Security Controls**

941 If security controls are not in place or are configured improperly, the process of establishing the

942 information exchange could expose the systems to access by unauthorized personnel. Therefore, the

943 first step is to implement appropriate security controls or to configure existing controls, as specified in

944 the agreement(s) and implementation plan. Security controls may include any of the controls from [\[SP](#)

945 [800-53\]](#) (based on risk assessment and system impact levels).

#### 947 **3.2.2.3 Integrate Applications**

948 Integrate applications or protocols for services that support the information exchange. Examples

949 include, but are not limited to, database applications, email, web browsers, application servers,

950 authentication servers, domain servers, development tools, editing programs, and communications

951 programs.

#### 953 **3.2.2.4 Conduct Operational and Security Testing**

954 Conduct an assessment to determine if the equipment that supports the information exchange operates

955 properly and that there are no obvious ways for unauthorized users to circumvent or defeat security

956 controls.<sup>8</sup> Test the interface between applications across the exchange, and simulate data traffic at

957 planned activity levels to verify correct translation at the receiving end. Test security controls under

958 realistic conditions. If possible, conduct testing in an isolated, non-operational environment to avoid

959 affecting the systems.

960 Document the results of the testing, and compare them with a set of predetermined operational and

961 security requirements approved by each organization. Determine whether the results meet a mutually

962 agreed level of acceptable risk and whether other actions are required. Correct weaknesses or

963 problems, and document the actions taken. Retest the exchange and implemented controls to ensure

964 that weaknesses or problems were eliminated and that new flaws have not been introduced.

965

966

---

<sup>8</sup> Operational and security assessments may be performed as part of ongoing risk management in accordance with [\[SP 800-37\]](#), [\[SP 800-53A\]](#), and [\[SP 800-137\]](#).



### 967 **3.2.2.5 Conduct Security Training and Awareness**

968 Conduct security training and awareness for all authorized personnel who will be involved in managing,  
969 using, or operating the information exchange. Provide training and awareness for new users and  
970 refresher training for all users periodically. Distribute the rules of behavior to all personnel who will be  
971 authorized to exchange information. Ensure that personnel know how to report suspicious or prohibited  
972 activity and how to request assistance if they encounter problems.

### 973 974 **3.2.2.6 Update System Security Plans**

975 The organizations update their system security plans and related artifacts to reflect the changed security  
976 environment in which their respective system operates. In addition, consider conducting mutual reviews  
977 of those sections of the updated plans that are relevant to the information exchange. The details for  
978 conducting mutual reviews are addressed in information exchange agreements.

979  
980 It is recommended that the security plans include the following information regarding the information  
981 exchange (and other information exchanges, if appropriate):

- 982 • Names of affected systems
- 983 • Participating organizations
- 984 • Method of exchange
- 985 • Names and titles of authorizing management officials
- 986 • Date of authorization
- 987 • Description/types of information to be exchanged
- 988 • Impact level of each type of information to be exchanged
- 989 • Impact level of affected systems
- 990 • Affected system interfaces
- 991 • Hardware inventory
- 992 • Software inventory
- 993 • Security concerns and rules of behavior governing the information exchange.

994 See [\[SP 800-18\]](#), *Guide for Developing Security Plans for Federal Information Systems*, for more  
995 information.

### 996 997 **3.2.2.7 Conduct Security Assessment and Authorization Activities**

998 Establishing an information exchange may represent a significant change to affected systems. Before  
999 proceeding further, each participating organization assesses and authorizes their respective system to  
1000 provide assurance that security protections remain at an acceptable level of risk. [\[SP 800-37\]](#) provides  
1001 information on assessment and authorization activities as part of the NIST Risk Management  
1002 Framework.

### 1003 1004 **3.2.3 Step 3: Activate the Information Exchange**

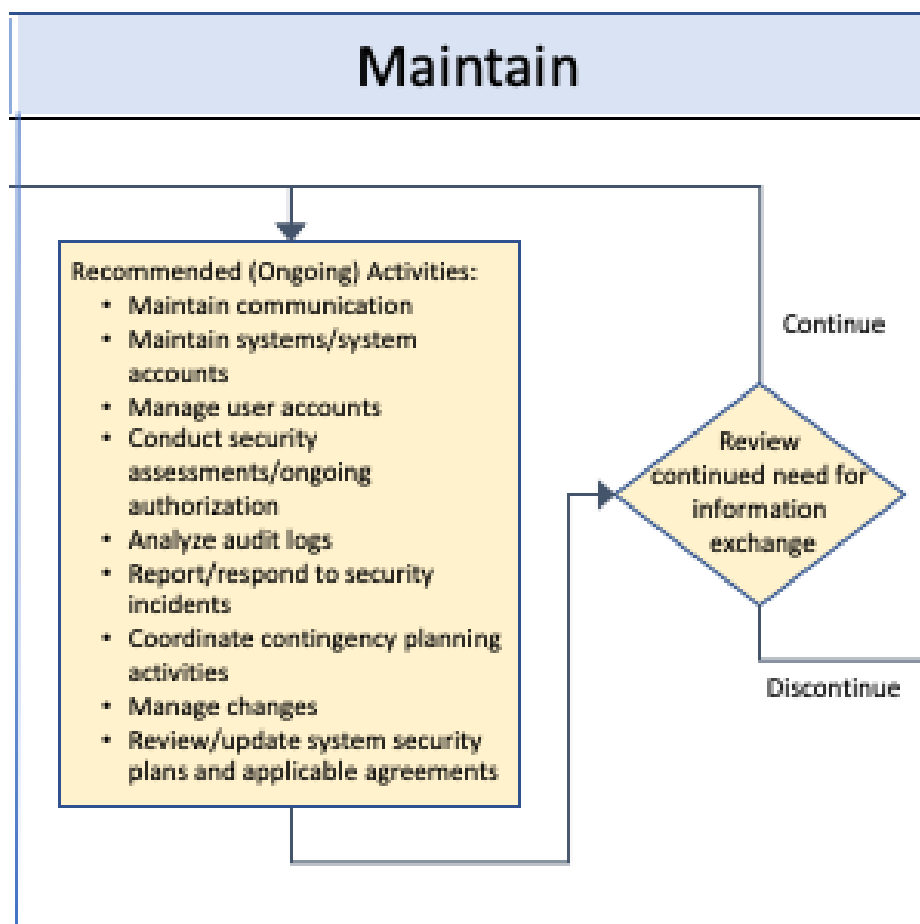
1005 Activate the information exchange for use by all parties, following prescribed guidelines. It is  
1006 recommended that the organizations closely monitor the information exchange for an agreed upon  
1007 period to ensure that it operates properly and securely. Analyze audit logs carefully and frequently, and  
1008 monitor the types of assistance requested by users. Document any weaknesses or problems that occur  
1009 and correct them.

1010

### 1011 3.3 Maintaining the Information Exchange

1012 Once established, the information exchange is actively maintained to help ensure that the information is  
 1013 exchanged securely. This section describes recommended activities for maintaining the information  
 1014 exchange, as shown in [Figure 5](#).

- 1015 • Maintain clear lines of ongoing communication.
- 1016 • Maintain systems and system components.
- 1017 • Manage user accounts
- 1018 • Conduct security assessments and ongoing authorization.
- 1019 • Analyze event logs.
- 1020 • Report and respond to security incidents.
- 1021 • Coordinate contingency planning activities.
- 1022 • Manage changes.
- 1023 • Review and update system security plans and applicable agreements.
- 1024 • Review continued need for the information exchange.



1025

1026

Figure 5: Information Exchange Maintain Phase

#### 1027 3.3.1 Maintain Clear Lines of Communication

1028 It is critical that the organizations participating in an information exchange maintain clear lines of  
 1029 communication and communicate regularly. Open lines of communication help to ensure that the

1030 information exchange and any associated interconnections are properly maintained and that security  
1031 controls remain effective. Open communications also facilitate change management activities by making  
1032 it easy for all sides to notify each other about planned system changes that could affect the information  
1033 exchange. Finally, maintaining clear lines of communication enables the organizations to promptly notify  
1034 each other of security incidents and system disruptions and to conduct coordinated responses.

1035  
1036 Communication between designated personnel is accomplished by using procedures specified in  
1037 agreements associated with the information exchange. Topics for communication include, but are not  
1038 limited to, the following:

- 1039 • Initial agreements and changes to agreements
- 1040 • Changes in designated management and technical personnel
- 1041 • Activities related to establishing and maintaining the information exchange
- 1042 • Changes to management activities that could affect the information exchange
- 1043 • Security incidents that could affect systems and data associated with the information  
1044 exchange
- 1045 • Contingencies that disrupt any of the systems associated with the information exchange
- 1046 • Termination of the information exchange
- 1047 • Planned restoration of the information exchange

1048

### 1049 **3.3.2 Maintain Systems and System Components**

1050 The participating organizations agree on the ownership and maintenance of any systems and system  
1051 components used to facilitate the information exchange. Systems and system components are  
1052 maintained in accordance with implemented controls from the [\[SP 800-53\]](#) Maintenance family.

1053

### 1054 **3.3.3 Manage User Accounts**

1055 User accounts associated with the information exchange are actively managed in accordance with  
1056 implemented controls from the [\[SP 800-53\]](#) Access Control, Identification and Authentication, and  
1057 Personnel Security families.

1058

### 1059 **3.3.4 Conduct Security Assessments**

1060 Security controls that support the information exchange are assessed with the frequency agreed to by  
1061 the participating organizations, whenever a significant change occurs, and/or in accordance with  
1062 organizational continuous monitoring programs to ensure that the controls are operating effectively and  
1063 are providing adequate protection.

1064

1065 Security assessments may be conducted by the designated audit authorities of one or all of the  
1066 participating organizations or by an independent third party. The organizations agree on the rigor of  
1067 reviews as well as processes for reporting and responding to assessment findings.

1068

1069 SPs [\[800-37\]](#), [\[800-53A\]](#), and [\[800-115\]](#), and [\[NISTIR 8011\]](#) provide guidance on conducting security  
1070 assessments. [\[SP 800-137\]](#) provides guidance on continuous monitoring.

1071

### 1072 **3.3.5 Analyze Event Logs**

1073 Event logs for systems and system components associated with the information exchange are analyzed

1074 with the frequency agreed upon by the participating organizations to detect and track unusual or  
1075 suspicious activities. Event logs are managed in accordance with implemented controls from the [\[SP](#)  
1076 [800-53\]](#) Audit and Accountability family. [\[SP 800-92\]](#) provides guidance on log management.  
1077

### 1078 **3.3.6 Report and Respond to Security Incidents**

1079 Organizations that participate in the information exchange notify each other of security incidents or  
1080 suspected security incidents that affect systems or system components associated with the information  
1081 exchange. The organizations then take appropriate steps to isolate and respond to such incidents in  
1082 accordance with their respective incident response procedures and implemented controls from the [\[SP](#)  
1083 [800-53\]](#) Incident Response family. Depending on the type and severity of the incident, organizations  
1084 may need to coordinate incident response activities or even terminate the information exchange. The  
1085 applicable agreements for the information exchange address the roles and responsibilities for incident  
1086 response for each participating organization, along with incident notification and emergency  
1087 termination processes. Incidents are reported in accordance with applicable laws, executive orders,  
1088 directives, regulations, policies, standards, and guidelines. SPs [\[800-61\]](#), [\[800-83\]](#), and [\[800-86\]](#) provide  
1089 guidance on incident response. Also see [\[US-Cert Federal Incident Notification Guidelines\]](#).  
1090

### 1091 **3.3.7 Coordinate Contingency Planning Activities**

1092 The organizations coordinate contingency planning training, testing, and exercises to minimize the  
1093 impact of disasters and other contingencies that could damage systems involved in the information  
1094 exchange or jeopardize the confidentiality, integrity, or availability of shared data. Give special attention  
1095 to emergency alerts and notifications, damage assessments, and response and recovery, including data  
1096 retrieval. The organizations may consider developing joint procedures based on existing contingency  
1097 plans, if appropriate. Finally, the organizations notify each other about changes to emergency POC  
1098 information (primary and alternate), including changes in staffing, addresses, telephone and fax  
1099 numbers, and e-mail addresses. [\[SP 800-34\]](#) provides guidance on contingency planning.  
1100

### 1101 **3.3.8 Manage Configuration Changes**

1102 Effective configuration management is critical to the maintenance and security of the information  
1103 exchange. Each organization establishes a change control board (CCB) or a similar body to review and  
1104 approve planned changes to its respective systems, such as upgrading software or adding services.

1105 The decision to upgrade or modify a system is based on the security requirements specified in applicable  
1106 agreements and a determination that the change will not adversely affect the exchange of information.  
1107 It is recommended that planned changes be tested in an isolated, non-operational environment to avoid  
1108 affecting systems. In addition, notify other parties of the changes in writing, and allow participating  
1109 organizations to be involved in the process.

1110 If a planned change is specifically applicable to the information exchange, participating organizations  
1111 establish a joint CCB or a similar body to review and approve the change. In most cases, such changes  
1112 are designed to improve the operation and security of the information exchange, such as by adding new  
1113 functions, improving user interfaces, and eliminating (or mitigating) known vulnerabilities. Nevertheless,  
1114 it is critical that organizations carefully review the changes before implementing them and manage and  
1115 track the changes after they are made. [\[SP 800-128\]](#) provides guidance on security-focused  
1116 configuration management.  
1117

**1118 3.3.9 Review and Maintain System Security Plans and Applicable Agreements**

1119 System security plans, applicable agreements (e.g., ISA, MOU/MOA, IEA, access agreements), and other  
1120 relevant documentation pertaining to the information exchange are reviewed and updated with a  
1121 frequency agreed to by the participating organizations or whenever there is a significant change to  
1122 systems associated with the information exchange. Refer to [\[SP 800-18\]](#) for information on updating  
1123 system security plans.

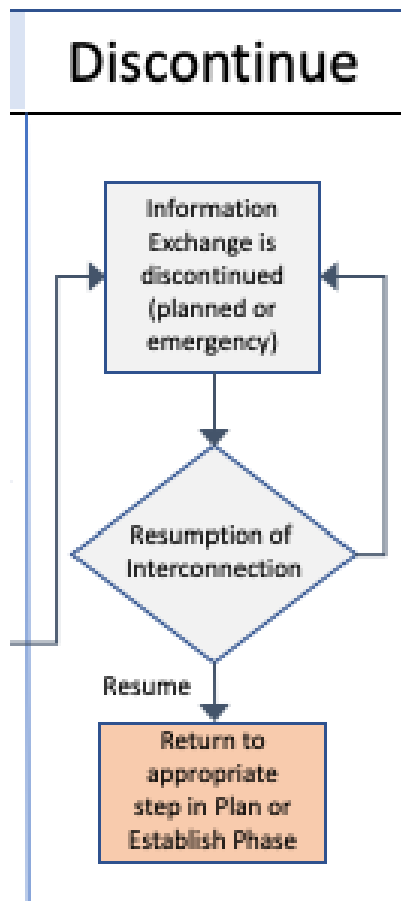
1124

**1125 3.3.10 Review the Continued Need for the Information Exchange**

1126 The business case for continuing the information exchange is reviewed with a frequency agreed to by  
1127 the participating organizations to determine if the exchange of information remains necessary. If the  
1128 information exchange is no longer necessary, [Section 3.4](#) provides information on discontinuing the  
1129 information exchange.

### 1130 3.4 Discontinuing the Information Exchange

1131 This section describes the process for discontinuing the information exchange, as shown in Figure 6. To  
 1132 the greatest extent possible, the information exchange is discontinued in a methodical manner to avoid  
 1133 system disruptions.



1134  
 1135 **Figure 6: Information Exchange Discontinue Phase**

#### 1136 3.4.1 Planned Discontinuance

1137 The decision to discontinue the information exchange involves appropriate managerial, security, and  
 1138 technical staff and is based on valid rationale, such as ongoing security failures by one or more  
 1139 participants or the lack of a mission-based need to continue the exchange. Before discontinuing the  
 1140 information exchange, the initiating party notifies the other parties in writing and waits to receive an  
 1141 acknowledgment in return. The notification describes the reasons for discontinuing the information  
 1142 exchange, provides the proposed timeline for the discontinuance, and identifies the technical and  
 1143 managerial staff who will conduct the discontinuance.

1144 An organization may have a variety of reasons to discontinue the information exchange, including:

- 1145 • Changed mission or business needs
- 1146 • Failed security assessments, including increases in risks that rise to unacceptable levels
- 1147 • Inability to abide by the technical specifications of agreements
- 1148 • Inability to abide by the terms and conditions of the agreements

- 1149           • Cost considerations, including increases in the cost of maintaining the exchange  
1150           • Changes in system configuration or in the physical location of equipment

1151 Schedule the discontinuance of the information exchange so that it permits a reasonable period for  
1152 internal business planning and allows participants to make appropriate preparations, including notifying  
1153 affected users and identifying alternative resources for continuing operations. In addition, managerial  
1154 and technical staff from each organization coordinate to determine the logistics of discontinuing the  
1155 information exchange and the disposition of shared data, including purging and overwriting moderate or  
1156 high impact data. Discontinue the information exchange when the impact on users is minimal, based on  
1157 known activity patterns. Following the discontinuance, each organization updates affected system  
1158 security plans and related documents to reflect the changed security environment in which its  
1159 respective systems operate.

### 1160 **3.4.2 Emergency Discontinuance**

1161 If a participating organization detects an attack, intrusion attempt, or other contingency that exploits or  
1162 jeopardizes the information or systems involved in the information exchange, it might be necessary to  
1163 abruptly terminate the information exchange without providing written notice to the other party. Such  
1164 an extraordinary measure is taken only in extreme circumstances and only after consultation with  
1165 appropriate technical staff and senior management.<sup>9</sup>

1166 The decision to make an emergency discontinuance is made by the system owner and implemented by  
1167 technical staff. If the system owner is unavailable, a predesignated staff member may authorize the  
1168 discontinuance in accordance with written criteria that stipulate the conditions under which this  
1169 authority can be exercised.

1170 The system owner or designee immediately notifies the other party's emergency contact by telephone  
1171 or other verbal method and receives confirmation of the notification. All parties work together to isolate  
1172 and investigate the incident in accordance with incident response procedures, including conducting a  
1173 damage assessment and reviewing audit logs and security controls. If the incident was an attack or an  
1174 intrusion attempt, the parties notify the relevant law enforcement authorities and make every attempt  
1175 to preserve evidence.

1176 After the emergency discontinuance, the initiating party provides a written notification to the other  
1177 party in a timely manner. The notification describes the nature of the incident, explains why the  
1178 information exchange was discontinued, describes how the information exchange was terminated, and  
1179 identifies actions taken to isolate and investigate the incident. In addition, the notification may specify  
1180 when and under what conditions the information exchange may be restored.

### 1181 **3.4.3 Resumption of Interconnection**

1182 The organizations may choose to resume the information exchange after it has been discontinued. The  
1183 decision to resume the information exchange is based on the cause and duration of the discontinuance.  
1184 For example, if the information exchange was discontinued because of an attack, intrusion, or other  
1185 contingency, all parties implement appropriate countermeasures to prevent a recurrence of the

---

<sup>9</sup> Each organization should consult with its legal counsel well in advance of a potential emergency disconnection in order to address issues related to liability, investigation, and evidence preservation.

1186 problem and modify agreements to address any issues that require attention. Alternatively, if the  
1187 information exchange has been discontinued for a long period of time (e.g., several months or more),  
1188 each party performs a risk assessment on its respective system and reexamines all relevant planning and  
1189 implementation issues, including the development of new agreements.



## References

### REGULATIONS, DIRECTIVES, PLANS, AND POLICIES

- [DHS BOD 18-02] Department of Homeland Security (2018) Securing High Value Assets. (U.S. Department of Homeland Security, Washington, D.C.), Binding Operational Directive 18-02, May 7, 2018.  
Available at <https://cyber.dhs.gov/bod/18-02/>
- [OMB A-130] Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016.  
<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf>

### STANDARDS, GUIDELINES, AND REPORTS

- [FIPS 140-3] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3.  
<https://doi.org/10.6028/NIST.FIPS.140-3>
- [FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 199.  
<https://doi.org/10.6028/NIST.FIPS.199>
- [SP 800-18] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-18r1>
- [SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-30r1>
- [SP 800-34] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010.  
<https://doi.org/10.6028/NIST.SP.800-34r1>
- [SP 800-35] Grance T, Hash J, Stevens M, O'Neal K, Bartol N (2003) Guide to Information Technology Security Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-35.

- <https://doi.org/10.6028/NIST.SP.800-35>
- [SP 800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2.  
<https://doi.org/10.6028/NIST.SP.800-37r2>
- [SP 800-50] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50.  
<https://doi.org/10.6028/NIST.SP.800-50>
- [SP 800-52] McKay KA, Cooper DA (2019) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-52, Rev. 2.  
<https://doi.org/10.6028/NIST.SP.800-52r2>
- [SP 800-53] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020.  
<https://doi.org/10.6028/NIST.SP.800-53r5>
- [SP 800-53A] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014.  
<https://doi.org/10.6028/NIST.SP.800-53Ar4>
- [SP 800-53B] Joint Task Force (2020) Control Baselines for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B, Includes updates as of December 10, 2020.  
<https://doi.org/10.6028/NIST.SP.800-53B>
- [SP 800-60-1] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-60v1r1>
- [SP 800-60-2] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1.

- <https://doi.org/10.6028/NIST.SP.800-60v2r1>
- [SP 800-61] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2.  
<https://doi.org/10.6028/NIST.SP.800-61r2>
- [SP 800-77] Barker EB, Dang QH, Frankel SE, Scarfone KA, Wouters P (2020) Guide to IPsec VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-77, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-77r1>
- [SP 800-83] Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for Desktops and Laptops. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-83, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-83r1>
- [SP 800-86] Kent K, Chevalier S, Grance T, Dang H (2006) Guide to Integrating Forensic Techniques into Incident Response. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-86.  
<https://doi.org/10.6028/NIST.SP.800-86>
- [SP 800-92] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92.  
<https://doi.org/10.6028/NIST.SP.800-92>
- [SP 800-113] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-113.  
<https://doi.org/10.6028/NIST.SP.800-113>
- [SP 800-115] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115.  
<https://doi.org/10.6028/NIST.SP.800-115>
- [SP 800-128] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates as of October 10, 2019.  
<https://doi.org/10.6028/NIST.SP.800-128>
- [SP 800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards

and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137.  
<https://doi.org/10.6028/NIST.SP.800-137>

- [SP 800-181] Petersen R, Santos D, Wetzel KA, Smith MC, Witte GA (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1.  
<https://doi.org/10.6028/NIST.SP.800-181r1>
- [IR 8011-1] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 1: Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Vol. 1.  
<https://doi.org/10.6028/NIST.IR.8011-1>
- [IR 8011-2] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Vol. 2.  
<https://doi.org/10.6028/NIST.IR.8011-2>
- [IR 8011-3] Dempsey KL, Eavy P, Goren N, Moore G (2018) Automation Support for Security Control Assessments: Software Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Vol. 3.  
<https://doi.org/10.6028/NIST.IR.8011-3>
- [IR 8011-4] Dempsey KL, Takamura E, Eavy P, Moore G (2020) Automation Support for Security Control Assessments: Software Vulnerability Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Vol. 4.  
<https://doi.org/10.6028/NIST.IR.8011-4>

#### MISCELLANEOUS PUBLICATIONS AND WEBSITES

- [HVA Control Overlay] Cybersecurity & Infrastructure Security Agency (2021) *High Value Asset Control Overlay*.  
 Available at <https://www.cisa.gov/publication/high-value-asset-control-overlay>
- [NARA CUI] National Archives and Records Administration (2020) *Controlled Unclassified Information (CUI) Registry*.  
 Available at <https://www.archives.gov/cui>
- [NIST NICE] National Institute of Standards and Technology (2020) *National Initiative for Cybersecurity Education (NICE)*.  
 Available at <https://www.nist.gov/itl/applied-cybersecurity/nice>

[USCERT IR]      Cybersecurity & Infrastructure Security Agency, *US-CERT Federal Incident Notification Guidelines*, April 2017.  
<https://us-cert.cisa.gov/incident-notification-guidelines>

1191

1192

## Appendix A—Glossary

acceptable use agreement	See <i>user agreement</i> .
access agreement	See <i>user agreement</i> .
application interconnection	A logical communications link between two or more applications operated by different organizations or within the same organization but within different authorization boundaries used to exchange information or provide information services (e.g., authentication, logging).
electronic/digital file transfer	An electronic or digital file transfer is the transmission of a file (information) between two systems via a file transfer (communications) protocol.
file sharing services	File sharing services include, but are not limited to, information sharing and access to information via web-based file sharing or storage.
information exchange	Access to or the transfer of data outside of system authorization boundaries in order to accomplish a mission or business function.
information exchange agreement	An information exchange agreement (IEA) is a document that specifies protection requirements and responsibilities for information being exchanged outside of system authorization boundaries. The IEA is similar to the ISA but does not include technical details associated with an interconnection.
interconnection	See <i>system interconnection</i> .
interconnection security agreement	An interconnection security agreement (ISA) is a document that specifies information security requirements for system interconnections, including the security requirements expected for the impact level of the information being exchanged for all participating systems.
intermittent ad-hoc connection	An intermittent, ad-hoc connection is a needs-based connection that is initiated for a specific time or purpose after which the connection is terminated. Intermittent connections are most often made via virtual connection.
memoranda of understanding/agreement	A memoranda of understanding/agreement (MOU/MOA) is a statement of intent between the participating organizations to work together and often states goals, objectives, or the purpose for the partnership; details the terms of and conditions for the agreement; and outlines the operations needed to achieve the goals or purpose.
network interconnection	A physical or virtual communications link between two or more networks operated by different organizations or operated within the same organization but within different authorization boundaries.
non-disclosure agreement	A non-disclosure agreement (NDA) delineates specific information, materials, or knowledge that the signatories agree not to release or divulge to any other parties.

permanent connection	A permanent connection is a perpetual communication channel. Permanent connections are most often made via a dedicated circuit.
service-level agreement [SP 800-35]	A service-level agreement (SLA) represents a commitment between a service provider and one or more customers and addresses specific aspects of the service, such as responsibilities, details on the type of service, expected performance level (e.g., reliability, acceptable quality, and response times), and requirements for reporting, resolution, and termination.
scheduled data transfer	A scheduled data transfer is a connection used to transfer data on a regular, recurring basis.
system interconnection	A system interconnection is a direct connection between two or more systems in different authorization boundaries for the purpose of exchanging information and/or allowing access to information, information services, and resources.
user agreement	User agreements, access agreements, and acceptable use agreements are user-based agreements that are similar to rules of behavior and specify user responsibilities when exchanging information or accessing information or systems that contain the exchanged information.

**Appendix B—Acronyms and Abbreviations**

AO	Authorizing Official
BOD	Binding Operational Directive
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standard
FTPS	File Transfer Protocol Secure
GRC	Governance, Risk, and Compliance
HTTPS	Hypertext Transfer Protocol Secure
HVA	High Value Asset
IEA	Information Exchange Agreement
IPSec	Internet Protocol Security
ISA	Interconnection Security Agreement
ISP	Internet Service Provider
IT	Information Technology
L2TP	Layer Two Tunneling Protocol
MOU/A	Memorandum of Understanding/Agreement
NARA	National Archives and Records Administration
NDA	Non-disclosure Agreement
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report



OMB	Office of Management and Budget
RE(f)	Risk Executive Function
RMF	Risk Management Framework
SCP	Secure Copy Protocol
SP	Special Publication
SSL	Secure Sockets Layer
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241

## Appendix C—Agreement Templates and Guidance

### Example Information Exchange Agreement<sup>10</sup>

**PURPOSE:** The purpose of this Information Exchange Agreement (IEA) is to establish the terms, conditions, and safeguards under which [specify organization] will disclose to [specify organization] certain information, records, or data to [state reason for IEA]. By entering into this IEA, the [specify organization] agrees to comply with the terms and conditions set forth in [specify location of terms or conditions] and all other terms and conditions set forth in this IEA.

#### PROGRAMS, INFORMATION EXCHANGE, AND SYSTEMS:

- The [specify organization] will use data received or accessed from [specify organization] under this IEA for the purpose of [specify purpose of the information exchange].
- The [specify organization] will use the information **only** for the specified purpose for which access to the [information, system, or both] is granted. In particular, the [specify organization] will use: [specify information type disclosed by [specify organization] only to [specify purpose]].

**DOCUMENT SUBMISSION:** Prior to signing this IEA, the [specify organization] will complete and submit to [specify organization] [specify submission requirements, if any].

**TRANSFER OF DATA:** [Specify organization] will provide the information to the [specify organization] under this IEA using the following information exchange method: [Specify method(s) of transfer, such as system interconnection, electronic/digital file transfers, portable storage device(s), or other method approved by [specify organization]].

**SECURITY PROCEDURES:** The [specify organization] will comply with [specify applicable federal laws, executive orders, directives, regulations, policies, standards, and guidelines]. In addition, the [specify organization] will comply with the following [specify organization-specific regulations, policies, procedures, etc.].

**RECEIVING ORGANIZATION'S RESPONSIBILITIES:** The [specify organization] is responsible for: [specify receiving organization's responsibilities].

**CONTRACTOR/AGENT RESPONSIBILITIES:** The [specify organization] will restrict access to the information obtained from [specify organization] to only those authorized [specify organization] employees, contractors, and agents who need such information to perform official duties as specified by purposes identified in this IEA. In addition, the [specify organization] will comply with the limitations on the use, duplication, and redisclosure of [specify organization] information set forth in [specify any additional agreement, policy, etc.] with respect to its contractors and agents.

1. The [specify organization] will ensure that its employees, contractors, and agents:
  - a. Properly safeguard [information types] furnished by [specify organization] under this IEA from loss, theft, or inadvertent disclosure;
  - b. Understand that they are responsible for safeguarding [specify information types] at all times, regardless of whether or not the [specify organization] employee,

---

<sup>10</sup> This example agreement is not intended to be used as a legal document. Organizations are advised to seek legal advice before finalizing and signing Information Exchange Agreements.

- 1242 contractor, or agent is at their regular duty station;
- 1243 c. Ensure that laptops, portable storage devices, and any other electronic devices or
- 1244 media containing [specify information types] are protected as specified by [specify
- 1245 organization] (e.g., encrypted); and
- 1246 d. Send emails or otherwise transmit [specify information types] only if protected
- 1247 as specified by [specify organization] (e.g., encrypted). (Note that organizations
- 1248 may specify that some or all exchanged information **cannot** be transmitted to
- 1249 organizations not party to this agreement.)
- 1250
- 1251 2. If an employee of the [specify organization] or an employee of the [specify organization's]
- 1252 contractor or agent becomes aware of a suspected or actual loss or breach of [specify
- 1253 information types], the [specify organization] must notify [specify organizational roles to be
- 1254 notified] within [specify time period] of suspected or actual loss or breach awareness.
- 1255
- 1256 3. [Specify organization] will report the information loss or breach of data in accordance
- 1257 with federal and [specify organizational] policies and procedures.
- 1258
- 1259 4. If the [specify organization] experiences a loss or breach of data, it will provide notice to
- 1260 individuals whose data has been lost or breached in accordance with [specify applicable
- 1261 federal laws, executive orders, directives, regulations, policies, standards, and guidelines]
- 1262 and bear any costs associated with the notice or any mitigation.
- 1263

1264 **POINTS OF CONTACT:** Specify points of contact for each organization. Different points of contact may  
 1265 need to be specified for different issues (e.g., information exchange issues, program or policy issues,  
 1266 system issues, system security issues, agreement issues, technical issues, incident response, etc.).

1267 **DURATION:** The effective date of this IEA is [specify date]. This IEA will remain in effect [specify  
 1268 time- and/or event-driven triggers for duration].

1269 **CERTIFICATION AND PROGRAM CHANGES:** At least [specify time period] before the expiration of  
 1270 this IEA, the [specify organization] will certify in writing to [specify organization] that: (1) it is in  
 1271 compliance with the terms and conditions of this IEA; (2) the information exchange processes under  
 1272 this IEA have been and will continue to be conducted without change; and (3) upon [specify  
 1273 organization]'s request, provide event logs, assessment reports, or other documents that demonstrate  
 1274 review and oversight activities. If there are substantive changes in any of the programs or information  
 1275 exchange processes listed in this IEA, the parties will modify the IEA accordingly.

1276 **MODIFICATION:** Modifications to this IEA must be in writing and agreed to by all parties.

1277 **TERMINATION:** The parties may terminate this IEA at any time upon mutual written consent. In  
 1278 addition, either party may unilaterally terminate this IEA upon [specify time period] advance written  
 1279 notice to the other party. Such unilateral termination will be effective [specify time period] after the  
 1280 date of the notice or at a later date specified in the notice. [Specify organization] may immediately  
 1281 suspend the information exchange under this IEA or terminate this IEA if [specify organization], in its  
 1282 sole discretion, determines that the [specify organization] (including its employees, contractors, and  
 1283 agents) has: (1) made an unauthorized use or disclosure of [specify organization]-supplied data or  
 1284 (2) violated or failed to follow the terms and conditions of this IEA or the other agreement(s).

1285 **AUTHORIZED SIGNATURES:** The signatories below warrant and represent that they have  
 1286 competent authority on behalf of their respective organizations to enter into the obligations in this IEA.

1291 [Specify Organizational Official]

1292 [Specify Organizational Official]

1293 \_\_\_\_\_  
 1294 (Signature Date)

\_\_\_\_\_  
 (Signature Date)

## EXAMPLE INTERCONNECTION SECURITY AGREEMENT<sup>11</sup>

1295  
1296  
1297

### SECTION 1: INTERCONNECTION STATEMENT OF REQUIREMENTS

1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306

The requirements for interconnection between [specify organization] and [specify organization] are for the express purpose of exchanging data between [specify system to be interconnected] owned by [specify organization] and [specify system to be interconnected] owned by [specify organization]. [Specify organization] requires the use of [specify organization]'s [specify system to be interconnected], and [specify organization] requires the use of [specify organization]'s [specify system to be interconnected] as approved and directed by [insert appropriate approving official] dated [specify date]. The expected benefit of the specified interconnection is to [specify benefits of the interconnection].

1307

### SECTION 2: SYSTEM SECURITY CONSIDERATIONS

1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
  
1335  
1336  
1337  
1338  
1339  
1340

- **General Information/Data Description.** [Describe the interconnection, whether it is a one- or two-way path, and the specific purpose of the interconnection].
- **Services Offered.** [Specify services provided by the interconnection, such as any user services that are offered, or specify that no services are offered and the limitations of the interconnection].
- **Information Types to Be Exchanged.** The types of information to be exchanged are as follows: [list all types of information that are to be exchanged].
- **Information Impact Level.** The impact levels of the information exchanged between [specify organization] and [specify organization] and the system categorization of the interconnected systems are as follows: [insert impact levels of the information types and the categorization of the systems involved in the interconnection].
- **User Community.** [Define any requirements for users, such as citizenship, background investigation, or other screening requirements].
- **Information Exchange Security.** [Describe specific security requirements to protect the information in accordance with information impact levels, system categorization, and organizational policy, such as "The use of FIPS 140-approved encryption mechanisms is required, and connections at each end must be located within controlled access facilities and guarded 24 hours a day. Individual users must have a need to know and have access to the information only through systems that have been authorized to operate in accordance with OMB Circular A-130. All access is controlled by agreed-upon authentication methods to validate the approved users." Requirements to implement specific SP 800-53 security controls or a specific SP 800-53B baseline may also be specified.]
- **Trusted Behavior Expectations.** [Specify organization]'s [specify system/information] and users are expected to protect [specify organization]'s [specify system/information], and [specify organization]'s [specify system/information] and users are expected to protect [specify organization]'s [specify system/information], in accordance with [list laws, regulations, executive orders, policies, standards, and guidelines].

---

<sup>11</sup> This example agreement is not intended to be used as a legal document. Organizations are advised to seek legal advice before finalizing and signing Interconnection Security Agreements.



## 1370 **Memorandum of Understanding/Agreement Development Guide**

1371 The organizations that own and operate the connected systems establish an MOU/A (or an equivalent  
1372 document) that defines the responsibilities of all parties in establishing, operating, and securing the  
1373 interconnection. The MOU/A is a management document that does not contain the technical details of the  
1374 interconnection. Those details are addressed separately in the ISA ([see above](#)).

1375 An MOU/A development guide is provided below, although organizations may use their own MOU/A  
1376 format. A sample MOU/A is provided below the development guide.

### 1377 **Supersession**

1378 Identify any previous agreements that this memorandum supersedes, including document titles and  
1379 dates. If the memorandum does not supersede any other agreements, so state.

### 1380 **Introduction**

1381 Use the Introduction section to describe the purpose of the memorandum. Identify the organizations and  
1382 systems that are involved in the interconnection.

### 1383 **Authorities**

1384 Identify any relevant legislative, regulatory, or policy authorities on which the MOU/A is based.

### 1385 **Background**

1386 Use the Background section to describe the systems that will be interconnected, the information that will  
1387 be exchanged or passed one way across the interconnection, and the business purpose for the  
1388 interconnection.

1389 Make the description of the systems brief and nontechnical. The goal is to identify the systems and their  
1390 authorization boundaries. The memorandum does not provide system specifications. The Background  
1391 section includes the formal name of each system, briefly describes system functions, identifies system  
1392 physical locations, identifies information impact or classification level and the system categorization or  
1393 classification level, and identifies the type(s) of information stored, processed, and/or transmitted by each  
1394 system.

### 1395 **Communications**

1396 Discuss the communications that will be exchanged between the parties throughout the duration of the  
1397 interconnection. Identify the specific events for which the parties must exchange formal notification, and  
1398 discuss the nature of such communications.

### 1399 **Interconnecting Security Agreement**

1400 State that the parties will jointly develop and sign an ISA before the systems can be connected. In  
1401 addition, describe the purpose of the ISA.

### 1402 **Security**

1403 State that all parties agree to abide by the security arrangements specified in the ISA. In addition, state  
1404 that all parties certify that their respective system is designed, managed, and operated in compliance with  
1405 all relevant federal laws, regulations, and policies.

**1406 Cost Considerations**

1407 The Cost Considerations section provides the financial details of the agreement. It specifies who will pay  
1408 for each part of the interconnection and the conditions under which financial commitments may be made.  
1409 Typically, each organization is responsible for the equipment necessary to interconnect its local system,  
1410 while the organizations jointly fund the interconnecting mechanism or media. However, the financial  
1411 arrangements are fully negotiable.

**1412 Timeline**

1413 Identify the expiration date of the memorandum and procedures for reauthorizing it. In addition, stipulate  
1414 that the memorandum may be terminated with written notice from one of the parties to the other. The  
1415 memorandum and the ISA have the same expiration date.

**1416 Signatory Authority**

1417 The memorandum includes a signature line with a signature block for each authorizing official. Arrange  
1418 the signature blocks on the same line: one signature on the left and one on the right. Include an area for  
1419 the date signed.

1420

## 1421 **Example Memorandum of Understanding/Agreement<sup>12</sup>**

1422  
1423

**SUPERSEDES:** (None or title and date of superseded document)

1424

### **INTRODUCTION**

1425  
1426  
1427  
1428  
1429  
1430  
1431

The purpose of this memorandum is to establish a management agreement between [specify organization] and [specify organization] regarding the development, management, operation, and security of an interconnection between [specify system] owned by [specify organization] and [specify system] owned by [specify organization]. This agreement will govern the relationship between [specify organization] and [specify organization], including designated managerial and technical staff, in the absence of a common management authority.

1432

### **AUTHORITY**

1433  
1434  
1435

The authority for this agreement is based on [specify document] issued by the [specify management official with appropriate authority] on [specify date of document authorizing the agreement].

1436

### **BACKGROUND**

1437  
1438  
1439  
1440  
1441  
1442  
1443

It is the intent of all parties to this agreement to interconnect systems to exchange data between [specify system] and [specify system]. [Specify organization] requires the use of [specify organization]'s [specify system], and [specify organization] requires the use of [specify organization]'s [specify system], as approved and directed by the [specify management official with appropriate authority] in [specify document named under "Authority" section]. The expected benefit of the interconnection is to [specify benefit(s) of the interconnection].

1444

Each system is described below:

1445  
1446  
1447  
1448  
1449  
1450

- **SYSTEM A**

- Name
- Function
- Location
- Description of information, including impact or classification level and system categorization

1451  
1452  
1453  
1454  
1455  
1456

- **SYSTEM B**

- Name
- Function
- Location
- Description of information, including impact or classification level and system categorization

1457

### **COMMUNICATIONS**

1458  
1459  
1460  
1461

Frequent formal communications are essential to ensuring the successful management and operation of the interconnection. The parties agree to maintain open lines of communication between designated staff at both the managerial and technical levels. All communications described herein must be conducted in writing unless otherwise noted.

1462  
1463

The owners of [specify system] and [specify system] agree to designate and provide contact information for technical leads for their respective systems and to facilitate direct

---

<sup>12</sup> This example agreement is not intended to be used as a legal document. Organizations are advised to seek legal advice before finalizing and signing Memorandum of Understanding/Agreement.



1464 contacts between technical leads to support the secure management and operation of the  
 1465 interconnection. To safeguard the confidentiality, integrity, and availability of the connected  
 1466 systems and the information that the systems store, process, and transmit, the parties  
 1467 agree to provide notice of specific events within the time frames indicated below:

- 1468 ▪ **Security Incidents:** Technical staff will immediately notify their designated  
 1469 counterparts by telephone or email when a security incident(s) is detected so that the  
 1470 other party may take steps to determine whether its system has been compromised  
 1471 and take appropriate security precautions. The system owner will receive formal  
 1472 notification in writing within [specify time period] after detection of the incident(s).  
 1473
- 1474 ▪ **Disasters and Other Contingencies:** Technical staff will immediately notify their  
 1475 designated counterparts by telephone or email in the event of a disaster or other  
 1476 contingency that disrupts the normal operation of one or all of the interconnected  
 1477 systems.  
 1478
- 1479 ▪ **Material Changes to System Configuration:** Planned technical changes to system  
 1480 architecture will be reported to technical staff before such changes are implemented.  
 1481 The initiating party agrees to conduct a risk assessment based on the new system  
 1482 architecture and to modify and re-sign the ISA within [specify time period] of  
 1483 implementation.  
 1484
- 1485 ▪ **New Interconnections:** The initiating party will notify the other party at least [specify  
 1486 time period] *before* an interconnected system is connected with any other system,  
 1487 including systems that are owned and operated by third parties.  
 1488
- 1489 ▪ **Personnel Changes:** The parties agree to provide notification of the separation or long-term  
 1490 absence of their respective system owner or technical lead. In addition, all parties will provide  
 1491 notification of any changes in point of contact information. All parties will also provide  
 1492 notification of changes to user profiles, including users who resign or change job  
 1493 responsibilities.

## 1494 INTERCONNECTION SECURITY AGREEMENT

1495 The technical details of the interconnection will be documented in an Interconnection  
 1496 Security Agreement (ISA). The parties agree to work together to develop the ISA, which  
 1497 must be signed by all parties before the interconnection is activated. Proposed changes to  
 1498 either system or the interconnecting medium will be reviewed and evaluated to determine  
 1499 the potential impact on the interconnection. The ISA will be renegotiated before changes  
 1500 are implemented. Signatories to the ISA shall be the Authorizing Official for each system.

## 1501 SECURITY

1502 All parties agree to work together to ensure the joint security of the interconnected systems  
 1503 and the information stored, processed, and transmitted, as specified in the ISA. Each party  
 1504 certifies that its respective system is designed, managed, and operated in compliance with  
 1505 all relevant federal laws, regulations, and policies.

## 1506 COST CONSIDERATIONS

1507 All parties agree to equally share the costs of the interconnecting mechanism and/or  
 1508 media, but no such expenditures or financial commitments shall be made without the  
 1509 written concurrence of all parties. Modifications to either system that are necessary to  
 1510 support the interconnection are the responsibility of the respective system owners'  
 1511 organization.

1512

**TIMELINE**

1513

This agreement will remain in effect for [specify time period] after the last date on either signature in the signature block below. After [specify time period], this agreement will expire without further action. If the parties wish to extend this agreement, they may do so by reviewing, updating, and reauthorizing this agreement. The newly signed agreement explicitly supersedes this agreement, which is referenced by title and date. If one or all parties wish to terminate this agreement prematurely, they may do so upon [specify time period] advanced notice or in the event of a security incident that necessitates an immediate response.

1514

1515

1516

1517

1518

1519

1520

1521

1522

**SIGNATORY AUTHORITY**

1523

I agree to the terms of this Memorandum of Understanding/Agreement.

1524

**[Specify Organizational Official]**

**[Specify Organizational Official]**

1525

1526

1527

\_\_\_\_\_  
(Signature      Date)

\_\_\_\_\_  
(Signature      Date)

1528