Draft NIST Special Publication 800-47 Revision 1

Managing the Security of Information Exchanges

Kelley Dempsey
Victoria Pillitteri
Andrew Regenscheid

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

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

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

Authority

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

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

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

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

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

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

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

Reports on Computer Systems Technology

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

Abstract

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

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

Keywords

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

Acknowledgments

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

Note to Reviewers

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

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

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

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

Call for Patent Claims

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

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

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

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

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

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

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

Such statements should be addressed to: sec-cert@nist.gov

Executive Summary

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

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

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

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

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

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

213
214 **Table of Contents**

List of Appendices

List of Figures

List of Tables

1 Introduction

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

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

1.1 Purpose and Applicability

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

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

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

1.2 Target Audience

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

1.3 Organization of this Publication

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

A References section provides references information. Appendix A provides glossary information. Appendix B provides acronym and abbreviation translations. Appendix C provides examples of some agreement types.

2 The Fundamentals

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

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

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

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

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

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

2.1 Types of Information Exchange

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

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

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

---

[1] A risk assessment includes the determination of threats, vulnerabilities, likelihoods, and impacts. See [SP 800-30] for additional information on conducting risk assessments.

[2] See [SP 800-37] for additional information on information security roles and responsibilities.

[3] [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.

2.1.1 System Interconnections

A system interconnection is defined as 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. An interconnection used for information exchange has at least three basic components: two (or more) endpoints and the mechanism by which the data flows (i.e., the "pipe" through which information is exchanged). The interconnection can be made from one location to another location or from one location to several locations. In this publication, it is assumed that the systems being interconnected are in different authorization boundaries, are owned and operated by different organizations, or are separately managed entities within the same organization. That is, management of the security of information exchanges is needed not only when information is exchanged between different organizations, but also when it is exchanged across authorization boundaries within a given organization.

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

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

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

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

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

- 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.

- 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

[4] For information on implementing secure VPNs, see [SP 800-77], *Guide to IPSec VPNs*, and [SP 800-113], *Guide to SSL VPNs*.

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

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

- Permanent (always on) Connection

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

- Scheduled Data Transfer

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

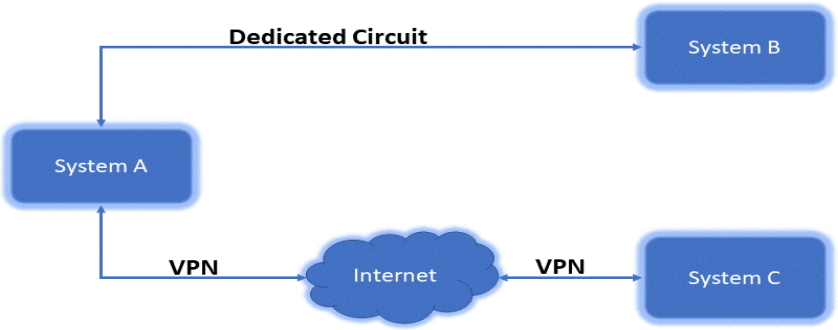
- Intermittent Ad-hoc Connection

  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.

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

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

[5] [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.

- 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.

2.2 Information Exchange: Accessing or Transferring the Information

Information may be exchanged by accessing or transferring the information using one or more more of the methods described in Section 2.1.

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

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

3 Information Exchange Security Management

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

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

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

The four phases of information exchange management are described below and depicted in Figure 2:

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

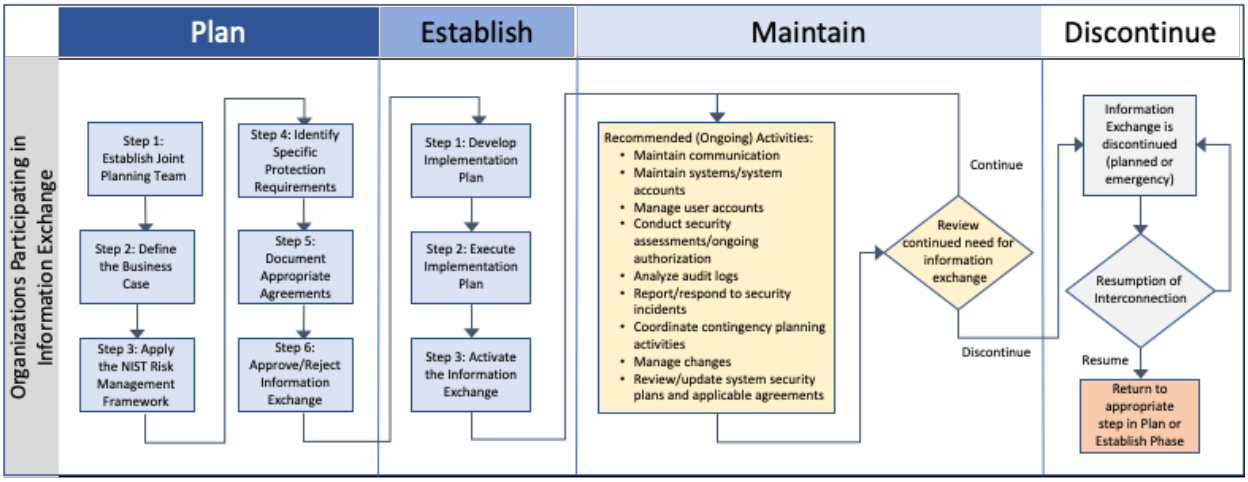


Figure 2: Phases of Information Exchange Management

3.1. Planning an Information Exchange

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

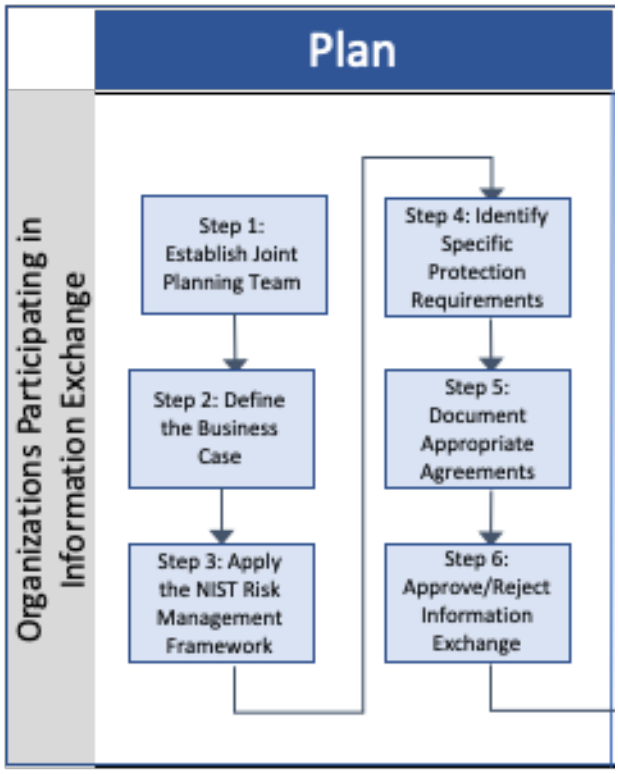


Figure 3: Information Exchange Planning Phase

3.1.1 Step 1: Establish a Joint Planning Team

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

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

3.1.2 Step 2: Define the Business Case

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

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

3.1.3 Step 3: Apply the NIST Risk Management Framework

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

3.1.4 Step 4: Identify Specific Protection Requirements

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

The joint planning team considers the following issues:

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

609 – Consider increased risk if data that has been designated as a High Value Asset (HVA)[6] is to
610 be exchanged.
611 – Consider the availablity 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

[6] 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.

future growth is anticipated. If new hardware is required, select products that are interoperable with existing hardware.

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

- *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

information. Coordinate disaster response training, testing, and exercises. Additional information on the Contingency Planning (CP) family of controls can be found in [SP 800-53]. [SP 800-34] provides detailed information on developing contingency plans.

- *Data Backup*: Determine backup and storage requirements for exchanged information. If backups are required, identify the types of information that require backup, the frequency of backups (e.g., daily, weekly, monthly), and which organization is responsible for the backups. Also, determine how to perform backups and how to link backups to contingency plan procedures. See controls in the Contingency Planning (CP) family (e.g., CP-6, *Alternate Site Storage,* and CP-9, *Information System Backup*) in [SP 800-53] for more specific guidance.
- *Configuration Management*: Determine how to coordinate the planning, design, and implementation of changes to the configuration baseline that could affect the security and functionality of the information exchange, such as upgrading hardware or software, changing configuration settings, or adding services. Establish a forum with relevant staff from each organization to review the proposed changes that may affect the information exchange. Coordinating configuration management activities reduces the potential for implementing changes that could introduce vulnerabilities or otherwise impact the confidentiality, integrity, or availability of the exchanged information or the systems processing, storing, or transmitting the information. Information on the Configuration Management (CM) family of controls is available in [SP 800-53]. [SP 800-128], *Guide for Security-Focused Configuration Management of Information Systems,* provides detailed information on configuration management.
- *Rules of Behavior*: Develop rules of behavior that clearly delineate the responsibilities and expected behavior of personnel authorized to access the exchanged information and the systems processing, storing, or transmitting the information. Document the rules in writing, and state the consequences of inconsistent behavior or noncompliance. Cover the documented rules of behavior in a security training and awareness program. See control PL-4, *Rules of Behavior*, in [SP 800-53].
- *Training and Awareness*: Define training and awareness requirements for personnel authorized to access the exchanged information and the systems processing, storing, or transmitting the information. The information exchange training and awareness requirements may be incorporated into existing training and awareness activities. Training and awareness requirements may include the frequency and scheduling of training and the assignment of responsibility for conducting training and awareness activities. Design training to ensure that personnel are familiar with the relevant policies, procedures, and rules of behavior associated with the exchanged information and the systems that process, store, or transmit the information. Require users to sign an acknowledgement form indicating an understanding of security responsibilities with regard to the information exchange, if appropriate. If shared applications are used, ensure that users know how to use them properly. Additional information on the Awareness and Training (AT) family of controls is available in [SP 800-53]. [SP 800-50] provides detailed information on building an information security awareness and training program. [SP 800-181] provides detailed information on a cybersecurity workforce framework. Additional information on information security education is available at the NIST National Initiative for Cybersecurity Education (NICE) website.

3.1.5 Step 5: Document Appropriate Agreements[7]

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

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

[7] [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**

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

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

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

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

The MOU/A are often applied to information exchanges in conjunction with an ISA. In general, an MOU 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. The MOA is most often used to address the financial responsibilities and obligations between the parties. While the MOA does not obligate funds, it could specify the authorities who can obligate funds. In support of information exchange, the MOU and MOA collectively address:

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

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

3.1.5.3 Information Exchange Agreement

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

3.1.5.4 Service-Level Agreement

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. Specific to information exchange and interconnections, SLAs explicitly address expectations regarding the ***availability*** of the connection used

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

3.1.5.5 User Agreement, Access Agreement, and Acceptable Use 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. User responsibilities addressed in the agreement may include, but are not limited to, what the user is permitted to do with the information, how the information is to be used, and whether the information can be transmitted to other parties. Users with access to the information read and sign the agreement to acknowledge acceptance and understanding prior to being given access to the information. The user, access, or acceptable use agreement may be specific to the information being exchanged, or the participating organizations may determine that existing agreements or rules of behavior already read and signed by participating organizational users provide sufficient protection.

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

3.1.5.6 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. An NDA may be valid for a defined time frame or may be indefinite.

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

3.1.5.7 Other Types of Agreements, Organization-Defined Agreement

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

3.1.5.8 Logged in Tracking System

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

3.1.6 Step 6: Approve or Reject the Information Exchange

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

- Approve the information exchange, or
- Reject the information exchange.

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

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

3.2 Establishing the Information Exchange

After the information exchange is planned and approved, it may be implemented. This section provides recommended steps for establishing the information exchange, as shown in Figure 4.

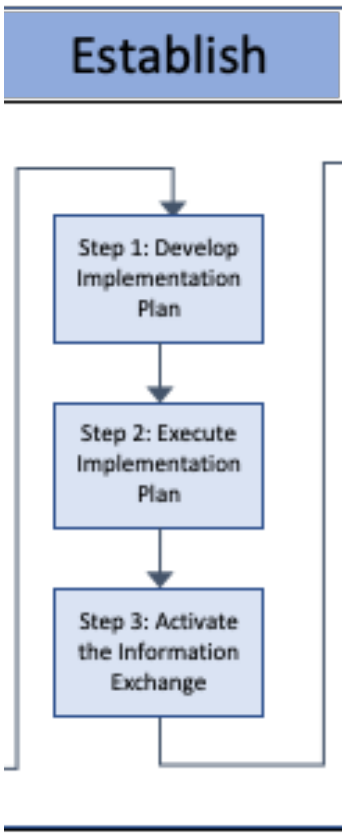


Figure 4: Information Exchange Establish Phase

3.2.1 Step 1: Develop an Implementation Plan

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

As appropriate, the implementation plan:

- Describes the systems involved in the information exchange
- Identifies the impact level of the information to be exchanged
- Identifies personnel responsible for establishing and maintaining the information exchange and specifies their responsibilities
- Identifies implementation tasks and procedures
- Identifies and describes security controls implemented to protect the confidentiality, integrity, and availability of the exchanged information
- 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.
939
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).
946
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.
952
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.[8] 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
961 Document the results of the testing, and compare them with a set of predetermined operational and
962 security requirements approved by each organization. Determine whether the results meet a mutually
963 agreed level of acceptable risk and whether other actions are required. Correct weaknesses or
964 problems, and document the actions taken. Retest the exchange and implemented controls to ensure
965 that weaknesses or problems were eliminated and that new flaws have not been introduced.
966

[8] 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].

3.2.2.5 Conduct Security Training and Awareness

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

3.2.2.6 Update System Security Plans

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

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

- Names of affected systems
- Participating organizations
- Method of exchange
- Names and titles of authorizing management officials
- Date of authorization
- Description/types of information to be exchanged
- Impact level of each type of information to be exchanged
- Impact level of affected systems
- Affected system interfaces
- Hardware inventory
- Software inventory
- Security concerns and rules of behavior governing the information exchange.

See [SP 800-18], *Guide for Developing Security Plans for Federal Information Systems,* for more information.

3.2.2.7 Conduct Security Assessment and Authorization Activities

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

3.2.3 Step 3: Activate the Information Exchange

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

3.3 Maintaining the Information Exchange

Once established, the information exchange is actively maintained to help ensure that the information is exchanged securely. This section describes recommended activities for maintaining the information exchange, as shown in Figure 5.

- Maintain clear lines of ongoing communication.
- Maintain systems and system components.
- Manage user accounts
- Conduct security assessments and ongoing authorization.
- Analyze event logs.
- Report and respond to security incidents.
- Coordinate contingency planning activities.
- Manage changes.
- Review and update system security plans and applicable agreements.
- Review continued need for the information exchange.

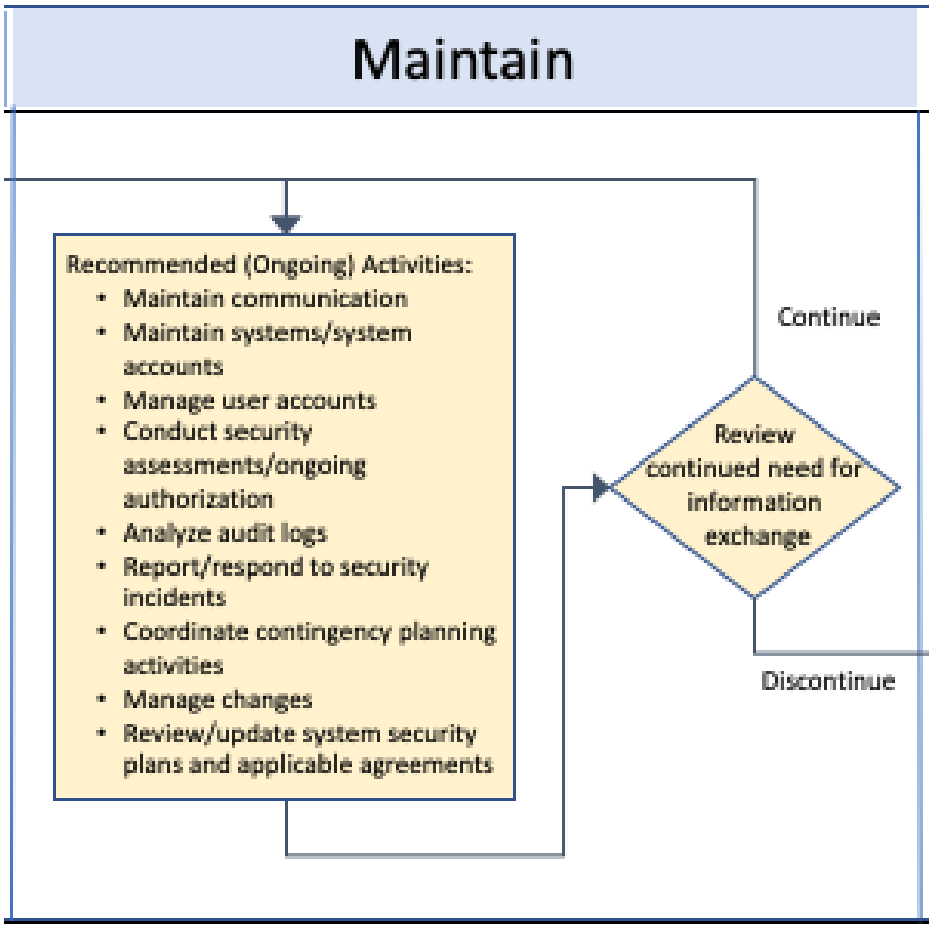


Figure 5: Information Exchange Maintain Phase

3.3.1 Maintain Clear Lines of Communication

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

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

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

- Initial agreements and changes to agreements
- Changes in designated management and technical personnel
- Activities related to establishing and maintaining the information exchange
- Changes to management activities that could affect the information exchange
- Security incidents that could affect systems and data associated with the information exchange
- Contingencies that disrupt any of the systems associated with the information exchange
- Termination of the information exchange
- Planned restoration of the information exchange

3.3.2 Maintain Systems and System Components

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

3.3.3 Manage User Accounts

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

3.3.4 Conduct Security Assessments

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

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

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

3.3.5 Analyze Event Logs

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

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

3.3.6 Report and Respond to Security Incidents

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

3.3.7 Coordinate Contingency Planning Activities

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

3.3.8 Manage Configuration Changes

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

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

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

3.3.9 Review and Maintain System Security Plans and Applicable Agreements

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

3.3.10 Review the Continued Need for the Information Exchange

The business case for continuing the information exchange is reviewed with a frequency agreed to by the participating organizations to determine if the exchange of information remains necessary. If the information exchange is no longer necessary, Section 3.4 provides information on discontinuing the information exchange.

3.4 Discontinuing the Information Exchange

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

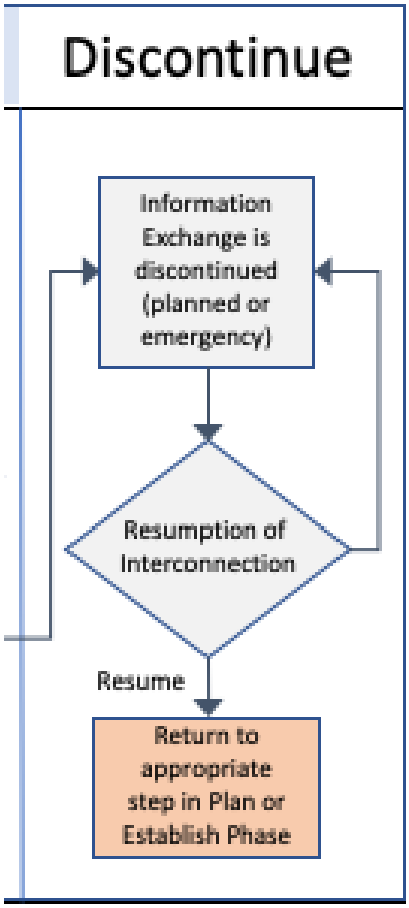


Figure 6: Information Exchange Discontinue Phase

3.4.1 Planned Discontinuance

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

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

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

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

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

3.4.2 Emergency Discontinuance

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

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

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

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

3.4.3 Resumption of Interconnection

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

[9] 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.

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

Appendix A—Glossary

acceptable use agreement	See *user agreement*.
access agreement	See *user agreement*.
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/digitial 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 *system interconnection*.
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 informtion, 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.

1193

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

1195

Appendix C—Agreement Templates and Guidance

Example Information Exchange Agreement[10]

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,

[10] 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.

contractor, or agent is at their regular duty station;

c. Ensure that laptops, portable storage devices, and any other electronic devices or media containing [specify information types] are protected as specified by [specify organization] (e.g., encrypted); and
d. Send emails or otherwise transmit [specify information types] only if protected as specified by [specify organization] (e.g., encrypted). (Note that organizations may specify that some or all exchanged information **cannot** be transmitted to organizations not party to this agreement.)

2. If an employee of the [specify organization] or an employee of the [specify organization's] contractor or agent becomes aware of a suspected or actual loss or breach of [specify information types], the [specify organization] must notify [specify organizational roles to be notified] within [specify time period] of suspected or actual loss or breach awareness.

3. [Specify organization] will report the information loss or breach of data in accordance with federal and [specify organizational] policies and procedures.

4. If the [specify organization] experiences a loss or breach of data, it will provide notice to individuals whose data has been lost or breached in accordance with [specify applicable federal laws, executive orders, directives, regulations, policies, standards, and guidelines] and bear any costs associated with the notice or any mitigation.

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

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

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

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

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

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

[Specify Organizational Official]	**[Specify Organizational Official]**
_____	_____
(Signature Date)	(Signature Date)

EXAMPLE INTERCONNECTION SECURITY AGREEMENT[11]

SECTION 1: INTERCONNECTION STATEMENT OF REQUIREMENTS

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].

SECTION 2: SYSTEM SECURITY CONSIDERATIONS

- **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].

[11] 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.

- **Formal Security Policy.** Policy documents that govern the protection of the interconnection and exchanged information are [specify organization]'s [specify policies] and [specify organization]'s [specify policies].

- **Incident Reporting.** The party that discovers a security incident will report it in accordance with federal and organization-specific incident reporting procedures. Any security incident associated with the interconnection or exchanged information will be reported to [specify reporting requirement details].

- **Event Logging.** [Specify organization and roles] are responsible for logging application processes and user activities that involve the interconnection. Activities that will be recorded include [list information to be captured by logs, such as event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers]. Event logs will be retained for [insert time period].

SECTION 3: TOPOLOGICAL DRAWING

(Insert a drawing here.)

SECTION 4: SIGNATORY AUTHORITY

This ISA is valid for [insert time period] after the last date on either signature below. At that time it will be updated, reviewed, and reauthorized. Either party may terminate this ISA with [specify time period] advanced notice in writing or in the event of a security incident that necessitates an immediate response.

[Specify Organizational Official]	**[Specify Organizational Official]**
_____	_____
(Signature Date)	(Signature Date)

Memorandum of Understanding/Agreement Development Guide

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

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

Supersession

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

Introduction

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

Authorities

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

Background

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

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

Communications

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

Interconnecting Security Agreement

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

Security

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

Cost Considerations

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

Timeline

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

Signatory Authority

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

Example Memorandum of Understanding/Agreement[12]

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

INTRODUCTION

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.

AUTHORITY

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].

BACKGROUND

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].

Each system is described below:

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

COMMUNICATIONS

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.

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

[12] 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.

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

- **Security Incidents:** Technical staff will immediately notify their designated counterparts by telephone or email when a security incident(s) is detected so that the other party may take steps to determine whether its system has been compromised and take appropriate security precautions. The system owner will receive formal notification in writing within [specify time period] after detection of the incident(s).

- **Disasters and Other Contingencies:** Technical staff will immediately notify their designated counterparts by telephone or email in the event of a disaster or other contingency that disrupts the normal operation of one or all of the interconnected systems.

- **Material Changes to System Configuration:** Planned technical changes to system architecture will be reported to technical staff before such changes are implemented. The initiating party agrees to conduct a risk assessment based on the new system architecture and to modify and re-sign the ISA within [specify time period] of implementation.

- **New Interconnections:** The initiating party will notify the other party at least [specify time period] *before* an interconnected system is connected with any other system, including systems that are owned and operated by third parties.

- **Personnel Changes:** The parties agree to provide notification of the separation or long-term absence of their respective system owner or technical lead. In addition, all parties will provide notification of any changes in point of contact information. All parties will also provide notification of changes to user profiles, including users who resign or change job responsibilities.

INTERCONNECTION SECURITY AGREEMENT

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

SECURITY

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

COST CONSIDERATIONS

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

TIMELINE

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.

SIGNATORY AUTHORITY

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

[Specify Organizational Official]	**[Specify Organizational Official]**
_____	_____
(Signature Date)	(Signature Date)