IT Security Procedural Guide: Managing Information Exchange Agreements CIO-IT Security-24-125

Initial Release

October 25, 2023

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – October 25, 2023		
N/A	McCormick/ Klemens/ Normand	nitial release to provide guidance on the types of information exchange agreements GSA uses and when to use them.	New Guide	N/A

APPROVAL

IT Security Procedural Guide: Managing Information Exchange Agreements, CIO-IT Security 24-125, Initial Release, is hereby approved for distribution.

DocuSigned by:

Bo Berlas

ED717926161544E...

Bo Berlas
GSA Chief Information Security Officer

For questions concerning GSA Policy and Compliance, contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.

Table of Contents

1 Introduction

National Institute of Standards and Technology Special Publication 800-47, Revision 1 (NIST SP 800-47, Revision 1), "Managing the Security of Information Exchanges" states:

> "When information is accessed or passed across the authorization boundary from one system to another, 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."

NIST SP 800-47, Revision 1 identifies potential agreement types that can be used to govern system information exchanges (see Appendix A).

Information exchanges and connections are addressed in NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations" controls CA-3, Information Exchange, and CA-9, Internal System Connections, and Sections 9-11 of the General Services Administration's (GSA) System Security and Privacy Plan (SSPP) templates. Section 9 is used to document an information system's authorization boundary with a system diagram depicting a system's connections and interconnections. Tables containing data about system interconnections are in tables in Section 11 of the SSPP.

1.1 Purpose

This guide identifies the type of agreements required for General Service Administration (GSA) systems for various types of information exchanges and the process for establishing the agreements and obtaining approval for them.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in establishing information exchange agreements for GSA systems and information. All GSA systems must adhere to the requirements and guidance provided regarding the procedures, processes, and methods for implementing information exchange agreements described in this guide. Per GSA Order CIO 2100.1, "a GSA system is a system:

- used or operated by GSA; or
- used or operated on behalf of GSA by a contractor of GSA or by another organization.

2 Definitions

The following definitions are from NIST SP 800-47, Revision 1.

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).

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 (IEA). A document specifying protection requirements and responsibilities for information being exchanged outside of system authorization boundaries. Similar to the interconnection security agreement but does not include technical details associated with an interconnection.

Interconnection security agreement (ISA). A document specifying information security requirements for system interconnections, including the security requirements expected for the impact level of the information being exchanged for all participating systems.

Interconnection/System interconnection. 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.

Memoranda of understanding/agreement (MOU/MOA). 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 following definitions are from CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts.

Internal information systems. Systems that reside on premise in GSA facilities and may connect to the GSA network. Internal systems are operated on behalf of GSA or the Federal Government (when GSA is the managing agency).

External information systems. Systems that reside in contractor facilities and typically do not connect to the GSA network. External information systems may be government owned and contractor operated or contractor owned and operated on behalf of GSA or the Federal Government (when GSA is the managing agency).

3 References

- FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems”
    - NIST SP 800-47, Revision 1, “Managing the Security of Information Exchanges”
    - NIST SP 800-53, Revision 5, “Security and Privacy Controls for Information Systems and Organizations”
    - CIO 2100.1, “GSA Information Technology (IT) Security Policy”

- CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk
- CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts

4 Identifying the Appropriate Exchange Agreement

The GSA's Office of the Chief Information Security Officer (OCISO) considered the information in NIST SP 800-47, Revision 1, GSA's IT operational environment, and GSA's organizational structure to determine what types of information exchange agreements are appropriate based on the following data.

- What type or method of exchanging information is used?
- Is the information exchange with an external or another internal system?
- Are the systems exchanging information under the purview of the same Authorizing Official (AO) or different (AOs)?
- What is the FIPS 199 Impact Level of the data involved (and therefore the resultant risk of that data being exposed)?
- Does the information exchanged include Personally Identifiable Information?

Based on the answers to the questions above, Table 4-1 can be used to determine if an information exchange agreement is required, and if so, the type of agreement required for a specific information exchange.

Table 4-1 identifies the documentation and agreement requirements for GSA systems. The documentation/agreement required and how the exchange is approved is based on the level and type of data exchanged, the type or method of exchange, and if the exchange is between GSA systems (internal) or between GSA and another entity's systems (external). Shaded cells in the table indicate that documenting information exchanges and connections in both systems SSPPs and having an approved ATO approves the information exchange.

Table 4-1. Information Exchange Agreements*

Exchange Type/Method	Examples	Internal/ External	AO Consideration	FIPS 199 Low Impact	FIPS 199 Moderate Impact	FIPS 199 High Impact
Exchage via email, portable media, or file transfer	Secure File Transfer Protocol (SFTP)	Internal	Same AO	None. Approved when SSPP/ATO is approved.	None. Approved when SSPP/ATO is approved.	None. Approved when SSPP/ATO is approved.
			Different AO	None. Approved when SSPP/ATO is approved.	None. Approved when SSPP/ATO is approved.	IEA/MOA
		External	N/A	IEA/MOA	IEA/MOA	IEA/MOA
Exchange via database or web-based services	Database, Web-based services Application Programming Interface (API).	Internal	Same AO	None. Approved when SSPP/ATO is approved.	None. Approved when SSPP/ATO is approved.	None. Approved when SSPP/ATO is approved.
			Different AO	None. Approved when SSPP/ATO is approved.	None. Approved when SSPP/ATO is approved.	IEA/MOA

Exchange Type/Method	Examples	Internal/ External	AO Consideration	FIPS 199 Low Impact	FIPS 199 Moderate Impact	FIPS 199 High Impact
		External	N/A	None. Approved when SSPP/ATO is approved.	None. Approved when SSPP/ATO is approved.	IEA/MOA
Exchange via system interconnection	Persistent connections (e.g., IPSec VPN, telecommunication circuits, etc.)	Internal	N/A	ISA/MOA	ISA/MOA	ISA/MOA
		External	N/A	ISA/MOA	ISA/MOA	ISA/MOA

* **Note 1**: ISA/MOA and IEA/MOA for external information exchanges may vary and align to the external organization requirements, when requested.
* **Note 2**: IEA/MOAs apply to specific system-to-system data exchanges. System-to-end-user data exchanges do not require such agreements (ex., an SFTP data transfer to or from an end user).

5 Information Exchange Agreement Templates

GSA has developed the following combined ISA/MOA and IEA/MOA templates for exchanges between internal systems and with external systems. The templates are available on the internal InSite IT Security Forms and Aids page. As noted in the table, agreements for external information exchanges may vary and align to the external organization requirements, when requested.

- Internal IEA-MOA Template
- Internal ISA-MOA Template
- External IEA-MOA Template
- External ISA-MOA Template

6 Maintaining Information Exchange Agreements

After an interconnection is established between systems, both participating organizations must continuously maintain the security of the systems, the information exchange, and the information exchanged. Information exchange agreements must be reviewed on an-agreed upon timeframe as documented in the agreement (typically annually) to verify that the requirements in the agreement are being met.

Changes to either system, the information exchange, or the configuration of the exchange method must be disclosed to the other party of the agreement and a determination made as to whether the agreement needs to be modified or a new agreement established.

Should either organization want to connect its information system with any other system, including third-party systems, the other party must by notified by an agreed upon time (typically 1 month) prior to the new connection.

7 Termination of Information Exchange Agreements

The parties to the agreement may terminate an information exchange agreement upon mutual written consent. Either party may terminate an agreement upon 30 days advanced notice. Either party may suspend an agreement if they determine that unauthorized use or disclosure of the exchanged data has occurred, or the terms and conditions of the agreement have not been followed. Communication among the parties to the agreement during an incident response may lead to an emergency suspension or termination of the agreement and reconsideration of the exchange after the incident has been resolved.

1. Appendix A. NIST SP 800-47, Revision 1, Reference Table

NIST SP 800-47, Revision 1 states:

> “The Potential Agreements Matrix (Table 1) [in the NIST SP] 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.”

Table A-1. Potential Agreements Matrix

	Low-Impact Information	Moderate-Impact Information	High-Impact Information
Exchange via email, 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