Homeland Security

U.S. Department of Homeland Security

DHS 4300A, "*Information Technology Security Program, Sensitive Systems*"

Attachment N

Preparation of Interconnection Security Agreements

Version 2.0

July 27, 2022

Protecting the Information that Secures the Homeland

This page intentionally blank

Document Change History

Version	Date	Description
1.0	April 28, 2022	Processes and authorities updated by Jeremy Tucker, Division Chief, Engineering, ITO
2.0	July 27, 2022	Adjudicated by OCIO CISOD Policy Office

CONTENTS

1.0 PURPOSE

This document provides the Department of Homeland Security (DHS) Components with information on the creation and use of Interconnection Security Agreements (ISAs). ISAs are vital in protection of the confidentiality, integrity, and availability of the data processed between interconnected IT systems.

Electronic connections between IT systems must be established in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, "Security Guide for Interconnecting Information Technology Systems." An ISA is required whenever the security policies of the interconnected systems are not identical, and the systems are not administered by the same Authorizing Official (AO). The ISA documents the security protections that must operate on interconnected systems to ensure that transmission between systems permits only acceptable transactions.

An ISA includes descriptive, technical, procedural, and planning information. It also formalizes the security understanding between the authorities responsible for the electronic connection between the systems.

An ISA must be reissued whenever a significant change occurs to any of the interconnected systems. Component personnel must review ISAs as part of the annual self-assessment required by the Federal Information Systems Management Act (FISMA). ISAs need not be reissued unless a significant system change has occurred, or three years have elapsed since its issuance.

2.0 BACKGROUND

A system interconnection is the direct connection of two or more information systems for the purpose of sharing data and other information resources by passing data between each other via a direct system-to-system interface without human intervention. Any physical connection that allows other systems to share data (pass thru) also constitutes an interconnection, even if the two systems connected do not share data between them. System interconnections include connections that are permanent in nature, connections that are established by automated scripts at prescribed intervals, and/or connections which utilize web and SOA services. System interconnections do not include instances of a user logging on to add or retrieve data, nor users accessing Web-enabled applications through a browser.

External connections are defined as system(s) or end points with an IP address that are not under the direct control of DHS, systems that have IP addressing not in the DHS addressing scheme (routable and non-routable), or systems that have an authorizing official who is not a DHS employee.

The foundations for this document are the sections on network connectivity in the *DHS* Management Directive 140-01*, "Information Technology Security Program"* and the amplifying document, *DHS* 4300A, *Information Technology Security Program, Sensitive Systems*," (hereafter known as DHS 4300A) and includes this document, Attachment N.

More detailed interconnection guidance is provided by NIST Special Publication (SP) 800-47, "Security Guide for Interconnecting Information Technology Systems." NIST SP 800-47 is the basis for ISA treatment in all three DHS documents.

3.0 SCOPE

This Instruction expands on the interconnection material in DHS Policy Directive 4300A, "*Information Technology System Security Program, Sensitive Systems*," and provides:

- A summary of the four interconnection phases defined in NIST SP 800-47: planning, establishing, maintaining an interconnection, and disconnecting
- More detail on ISA content
- A summary of two related documents defined in NIST SP 800-47: a Memorandum of Understanding or Agreement (MOU or MOA) and a System Interconnection Implementation Plan (SIIP).

Attachment N to the *DHS Policy Directive 4300A, Information Technology System Security Program, Sensitive Systems,"* applies to all DHS Components.

4.0 REFERENCES

Federal Laws

Federal Information Security Management Act of 2002, 44 USC 3541 et seq., enacted as Title III of the E-Government Act of 2002, Pub L 107-347, 116 Stat 2899

Office of Management and Budget (OMB) Memorandums

OMB Memorandum M-11-33, "FY 2011 Reporting Attachment for the Federal Information Security Management Act and Agency Privacy Management, Office of Management and Budget, M-11-33, September 14, 2011.

Department of Homeland Security Publications

DHS Management Directive 140-01*, "Information Technology Security Program*," Revision 2, May 5, 2017.

DHS Policy Directive 4300A*, "Information Technology System Security Program, Sensitive Systems," April 28, 2022.*

"Incident Response and Reporting," Attachment F to the *DHS 4300A, April 28, 2022*

"Vulnerability Assessment Program," Attachment O to the *DHS 4300A, April 28, 2022*

National Institute of Standards and Technology (NIST) Special Publications (SP)

NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," August 2002

NIST SP 800-53, Rev 5, "Recommended Security Controls for Federal Information Systems and Organizations," October 2020.

5.0 POLICY

The applicable network connectivity policy is located in the Access Control Section, for "Interconnection Security Agreements," of the DHS 4300A, *April 28, 2022.*

6.0 PROCEDURES

NIST SP 800-47 defines ISA development as just one in a sequence of coordination, planning, costing, and technical steps that are prerequisites for establishing and maintaining an operational interconnection. This section gives an outline of the steps. NIST SP 800-47 should be consulted for details, along with other guidelines and related DHS 4300A sections applicable to specific steps.

NIST SP 800-47 recognizes four life-cycle stages for an interconnection:

- Planning: Includes steps through ISA development and interconnection approval or rejection. These steps are directly relevant to this document.
- Establishing: Includes steps involving detailed technical preparations, culminating in a System Interconnection Implementation Plan (SIIP). (Although the SIIP comes after the ISA, Appendix N3 of this document includes a brief outline of the SIIP, since its topics include considerations pertinent to the planning stage).
- Maintaining: Includes routine security-relevant processes for the interconnection (e.g., security reviews, audit log analysis, contingency plan coordination) that are analogous to processes performed on the systems individually. This material is not covered in this document.
- Disconnecting: Includes processes for planned and emergency disconnections and for restoring a connection. This material is not covered in this document.

6.1 Steps in Planning an Interconnection

The planning steps are required. Their key components follow:

1. **Establish a joint planning team**:

- Form a combined managerial and technical staff, with support by system and data owners.
- The staff may serve beyond the planning phase to coordinate interconnection issues.
- Coordinate with IT capital planning, configuration management, and related activit

2. **Define the business case**:

- Define purpose, mission support, and potential costs, benefits, and risks.
- Consult with Privacy Officer and Legal Counsel to evaluate compliance with applicable regulations.

3. **Perform Security Authorization**:

- Perform security authorizations for the individual systems, or confirm that they are currently authorized to operate.
- For systems requiring a new or updated security authorization, develop required technical products in compliance with security authorization process guidance: Security Plan (SP), Risk Assessment (RA), Contingency Plan (CP), and security review.

4. Determine interconnection requirements:

- Conduct analysis required for ISA and development of Memorandum of Understanding (MOU) and Memorandym of Agreement (MOA) (in Step 5).
- Address the following issues[1]:
    - Level and method of interconnection
    - Impact on existing infrastructure and operations
    - Hardware requirements
    - Software requirements
    - Data sensitivity
    - User community
    - Services and applications
    - Security controls
    - Segregation of duties
    - Incident reporting and response
    - Contingency planning
    - Data element naming and ownership
    - Data backup
    - Change management
    - Rules of behavior
    - Security awareness and training
    - Roles and responsibilities
    - Scheduling
    - Costs and budgeting

5. **Document the interconnection agreement**:

- Produce the ISA and MOU or MOA
- Establish access controls for sensitive ISAs and for MOUs or MOAs

[1] The relevant considerations, more numerous than the outline of the ISA would suggest, also provide information for SIIP development in Stage 2.

6. Approve or reject the interconnection:

- Action Officer (AOs) (or officials designated by the AOs) review the ISA, MOU or MOA, and other relevant documentation, including the SIIP[2]
- Distribute copies of approved documents to responsible officials
- For an interim approval, AOs specify tasks remaining to be completed and schedules for these tasks
- For a rejected interconnection, return to the applicable planning steps

6.2 Steps in Establishing an Interconnection

The establishing steps identified by NIST SP 800-47 are the following[3]:

1. Develop a System Interconnection Implementation Plan (SIIP)

- Document the implementation plan following the SIIP outline given in Appendix C of NIST SP 800-47 (summarized in Appendix N3 of this document)[4]

2. Execute the implementation plan

- Implement or configure security controls in accordance with the SIIP. The brief discussions in NIST SP 800-47 (Section 4.2.1) of a variety of controls (e.g., firewalls, intrusion detection, auditing) identify applicable NIST SPs and some reminders (e.g., incorporating relevant control information into training)
- Install or configure hardware and software
- Integrate applications
- Conduct operational and security testing.
- Conduct security training and awareness.
- Update security plans.
- Perform a re-authorization through the security authorization process.

3. Establish the interconnection

7.0 RESPONSIBILITIES

The personnel responsibilities defined in the DHS 4300A, "*Information Technology Security Program, Sensitive Systems*" are the following:

[2] To review the SIIP in connection with determining approval implies that the establishing stage must precede at least Step 6, and in most cases Step 5, of the planning stage.

[3] Section 4 of NIST SP 800-47 provides useful discussion of these steps.

[4] The list of topics in Appendix C of NIST SP 800-47 is more comprehensive than the list given in the body of the document (Section 4.1). One topic cited in the body but not the appendix is the sensitivity of the data involved in the connection.

Person Responsible	Task
ISSMs	◦ Provide guidance and enforce management, operational, and technical controls that apply to network and system security configuration and monitoring. ◦ Evaluate the risks associated with external connections. ◦ Review programs and systems periodically to find out if changes have occurred that could adversely affect security.
AOs or Designated Official	◦ Review, approve, and sign the Interconnection Security Agreement (ISA). ◦ Ensure that ISAs are reissued every three years or whenever significant changes are made to any of the interconnected systems.
Program Officials	◦ Establish the requirement for the external connection and assess the associated risks.
Network Administrators	◦ Ensure technical controls governing use of the external connection remain in place and function properly. ◦ Assist in development of the ISA.
ISSOs	◦ Coordinate with the external agency in development of the ISA. ◦ Assist in preparation of the ISA and ensure all external connections are documented in the Security Plan, Risk Assessment, and security operating procedures. ◦ Review ISAs as a part of the annual FISMA self-assessment. ◦ Monitor compliance.
Users	◦ When connecting to DHS networks, ensure the equipment used to access these networks is protected from viruses and other malicious code and the protection software is kept current.

APPENDIX N1 - MEMORANDUM OF UNDERSTANDING OR AGREEMENT

A Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) defines the responsibilities for both parties in interconnecting, operating, and securing two systems. This brief nontechnical agreement is the authorization for detailed planning of an interconnection, leading to an ISA. NIST SP 800-47 allows use of organization-specific Memorandum formats but provides an example, based on the following outline:

Section 1: Supersession

Identify documents, if any, superseded by this MOU or MOA.

Section 2: Introduction

Identify the organizations and systems involved in the interconnection.

Section 3: Authorities

Identify relevant legislative, regulatory, or policy authorities on which the MOU or MOA is based.

Section 4: Background

Provide a nontechnical description of the proposed interconnection, including:

- business purpose to be served
- system functions
- system boundaries
- locations
- types of data affected by interconnection
- data sensitivity

Section 5: Communications

Discuss communications between the organizations and specific events requiring formal notifications. Technical communications information is confined to the ISA and the System Interconnection Implementation Plan (SIIP) (defined in Appendix N3.)

Section 6: Interconnection Security Agreement

State the agreement to develop and abide by an ISA, once approved. Identify the associated ISA if one already exists.

Section 7: Security

Confirm that the systems' designs, management, and operations comply with all applicable laws, regulations, and policies. State the agreement to abide by the security arrangements specified in the ISA, once approved.

Section 8: Cost Considerations

Identify the organizations' financial responsibilities for development, acquisition, and operation of the interconnected systems.

Section 9: Timeline

Identify the expiration date, procedures for MOU or MOA reauthorization, and the means of termination by either organization.

Section 10: Signatory Authority

The signatures of the organizations' authorized officials for the MOU/A and the dates of signing.

APPENDIX N2 - SYSTEM INTERCONNECTION IMPLEMENTATION PLAN

A System Interconnection Implementation Plan (SIIP) provides the technical detail needed to guide the development and establishment of an interconnection and thus to help both organizations confirm that all details have been covered. A SIIP supplements the associated MOU or MOA and ISA, agreements with more administrative than technical content. NIST SP 800-47 provides the following outline for a SIIP:

Section 1: Introduction

Section 2: System Interconnection Description

- 2.1 Security Controls
- 2.2 System Hardware
- 2.3 System Software
- 2.4 Data and Information Exchange
- 2.5 Services and Applications

Section 3: Roles and Responsibilities

Section 4: Tasks and Procedures

- 4.1 Implement Security Controls
- 4.2 Install Hardware and Software
- 4.3 Integrate Applications
- 4.4 Conduct a Risk Assessment
- 4.5 Conduct Operational Security and Testing
- 4.6 Conduct Security Training and Awareness

Section 5: Schedule and Budget

Section 6: Documentation

APPENDIX N3 INTERCONNECTION SECURITY AGREEMENT TEMPLATE

The following pages contain the preferred template for an ISA.

History of Changes to the Template

Version	Date	Description
1.0	January 22, 2022	Initial release

Homeland Security

Interconnection Security Agreement between

[Organization One] and

[Organization Two]

[System One]

And

[System Two]

Date

Securing Information that Protects the Homeland

Contents

{Copy this template into a new document. The section numbers should automatically start at 1.0 and run consecutively.

Create the Table of Contents when the Agreement is complete. The "Simple" Table of Contents provided by Microsoft Word is recommended, with page numbers right aligned and dot leaders.

Remove all italic guidance text.}

1.0 PURPOSE

This Interconnection Security Agreement (ISA) is required by Federal and Department of Homeland Security (DHS) policy and establishes individual and organizational security responsibilities for the protection and handling of unclassified information between the **[Organization 1]** and the **[Organization 2]**. Any specific requirements of both signatory organizations are also included.

2.0 Security Network Connectivity Policy

{Indicate what overall policy is providing the Security Network connectivity requirements and summarize the main requirements.}

{Sample} DHS Directive 140-01, "Information Technology Security Program (ITSP), Sensitive Systems" establishes DHS policy for network connectivity. The section on network connectivity states:

a. Components shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component.

b. Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnection security agreements.

c. Components shall document all interconnections to the DHS OneNetwork (OneNet) with an Interconnection Security Agreement (ISA), signed by the OneNet AO and by each applicable AO.

d. ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.

e. ISAs shall be reviewed and updated as needed as a part of the annual FISMA self-assessment..

f. Components may complete a master ISA, (which includes all transitioning systems) as part of their initial OneNet transition. After transition, each additional system or GSS shall be required to have a separate ISA. Interconnections between DHS Components (not including DHS OneNet) shall require an ISA whenever there is a difference in the security categorizations for confidentiality, integrity, and availability between the systems. ISAs shall be signed by each applicable AO.

g. The DHS CIO shall approve all interconnections between DHS information systems and non-DHS information systems. Components shall document interconnections with an ISA for each connection. The DHS CIO shall ensure that connections with other Federal Government Agencies are properly documented. A single ISA may be used for multiple connections provided that the security accreditation is the same for all connections covered by that ISA.

h. Components shall document interconnections between their own and external (Non-DHS) networks with an ISA for each connection.

i. The Department and Components shall implement Trust Zones through Policy Enforcement Points (PEP), as defined in the DHS Security Architecture.

j. DHS OneNet shall provide secure Name/Address resolution service. DNSSec has been designated as the DHS service solution.

k. All DHS systems connected to OneNet and operating at moderate or high level shall utilize secure Name/Address resolution service provided by DHS OneNet.

l. The appropriate CCB shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB.

2.1 ISA Requirements for Types of System Interconnections

System interconnections may be characterized as either direct or networked. Direct connections are single purpose point-to-point connections that support only the two connected systems. Directly connected systems do not rely on another network for their connectivity or security and are physically and electronically isolated from other networks and systems. Networked systems connect via an intervening network that exists as a general support system, not a single-purpose connection. Systems that are connected via an encrypted tunnel, whether on HSDN or any other network, are considered networked systems.

For networked U.S. Government systems, the ISA must include the owner and AO of the network as well as the owners of the applicable systems.

2.2 Scope

This interconnection security agreement addresses the interconnection of the **[Organization 1] [System 1 Name]** and the **[Organization 2] [System 2 Name]**. Additionally, the ISA covers application and/or control data traversing the networks.

2.3 Point of Contact (POC)

For all issues associated with this agreement, the established points of contact are as follows:

[Organization 1]	**[Organization 2]**
AO:	AO:
System Owner:	System Owner:
ISSO(s)	ISSO(s):
ISSM	ISSM
Program Manager	Program Manager

2.4 References

NIST Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems,* provides guidance in preparing and establishing connectivity between networks. NIST SP 800-47 specifies guidance for establishing network ISAs. The key points

are discussed in this ISA. Consult the full document for additional information and examples of ISAs and MOUs.

NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components of an information system that process, store, or transmit federal information.

- DHS Management Directive (MD) 140-01, "Information Technology Security Program."
- DHS Management Directive (MD) 140-01-001, "Information Technology Security Program (ITSP), Sensitive Systems"
- DHS, Type Accreditation, Attachment D to the DHS 4300A, "Information Technology Security Program, Sensitive Systems"
- DHS, Incident Response and Reporting, Attachment F to the DHS 4300A, "Information Technology Security Program, Sensitive Systems"
- DHS, Vulnerability Assessment Program, Attachment O to the DHS 4300A, "Information Technology Security Program, Sensitive Systems"
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems,
- NIST ITL Bulletin,, Secure Interconnections for Information Technology Systems
- NIST SP 800-53, Rev. 5, Recommended Security Controls for Federal Information.

3.0 INTERCONNECTION JUSTIFICATION

{Use this section to document the formal requirement(s) for connecting the two systems. Explain the rationale for the interconnection to the two AOs. Enter one or two narrative paragraphs that justify interconnecting the two systems being documented. Within the narrative information ensure that you include the following items:

1. *The names of the two systems being interconnected.*
2. *The requirement(s) for the interconnection to include the benefits derived.}*

{Sample} The requirements for interconnection between the two systems is for the express purpose of exchanging data between the **[Organization 1] [System 1 Name]** owned and operated by **[Organization 1]**, and the **[Organization 2] [System 2 Name]** owned by **[Organization 2]**. The **[Organization 2]** requires the use of **[Organization 1] [System 1 Name]** as a transport system for wide area network (WAN) services and interconnectivity to the DHS infrastructure. The expected benefit is to expedite the transfer and processing of data between DHS components and to reduce the overall WAN expenditures within the Department.

{Sample} The **[Organization 1] [System 1 Name]** is a DHS enterprise wide network designed to interconnect DHS Component Networks.

{Sample} The **[Organization 2] [System 2 Name]** interconnected with the **[Organization 1] [System 1 Name]** are **[Name 1]** LAN and **[Name 2]** LAN.

4.0 SECURITY CONSIDERATIONS

This section describes the security mechanisms in place to secure the connections between both systems. It outlines what the security considerations are and which organization is responsible for each. In some cases, both organizations will share security responsibility.

4.1 General Information/Data Description

{At a high level describe the purpose of the interconnection and the type of data contained within the systems.}

{Sample} The purpose of the interconnection between the **[Organization 1] [System 1 Name]** and the **[Organization 2] [System 2 Name]** is to interconnect DHS component networks to a single DHS WAN and provide a single trusted infrastructure. The data traversing the networks will include both **[Organization 1]** and **[Organization 2]** DHS unclassified operational and administrative data.

4.2 ISA Requirements Within and Across Organizational Boundaries

IT equipment within the boundary of the **[Organization 1] [System 1]** is owned, operated and maintained by **[Organization 1]** contracted services or government employees. All **[Organization 1]** IT equipment interconnected with the **[Organization 2] [System 2 Name]** will be hardened, at a minimum, per DHS 4300A hardening guidelines or specific waivers to hardening guidelines requested, documented, and approved by appropriate ISSM

IT equipment within the boundary of the **[Organization 2] [System 2 Name]** is owned, operated and maintained by **[Organization 2]** contracted services or government employees. All **[Organization 2] [System 2 Name]** IT equipment interconnected with the **[Organization 1] [System 1 Name]** will be hardened, at a minimum, per DHS 4300A hardening guidelines or per specific waivers to hardening guidelines requested, documented, and approved by appropriate ISSM.

[Organization 1] and the **[Organization 2]** shall protect the data in order to maintain confidentiality, integrity, and availability of the data and information systems. The data and information systems will be protected in accordance with DHS 4300A, "*Information Systems Security Program, Sensitive Systems*" the NIST SP 800-53 assigned minimum security controls, and FIPS 199 Security Categorization of both systems to ensure that the connection will be protected to the requirements of higher categorized system.

4.3 Physical Security and Environmental Controls

{Enter the specific requirements for providing physical security and environmental controls.}

{Sample} Physical Security, at a minimum, will be governed by DHS 4300A, "*Information Technology Security Programs, Sensitive Systems*," in the "Physical and Environmental Protection Control Family," and NIST SP 800-53 controls. Both organizations shall provide physical security and system environmental safeguards adequate to provide protection of the system components.

4.4 Data Sensitivity

{Enter the sensitivity or classification level of the information to be exchanged, in particular, the highest sensitivity (i.e., Privacy Act, Trade Secret Act, Law Enforcement Sensitive, Sensitive-But-Unclassified, etc.) or classification (Confidential, Secret, Top Secret) and most restrictive protection requirements for information to be handled through the interconnection.}

{Sample} The highest level of data that traverses the **[Organization 1] [System 1 Name]** is Sensitive but Unclassified (SBU). This may include, but is not limited to, Sensitive Personally Identifiable Information, For Official Use Only, financial, and/or Law Enforcement Sensitive data.

{Sample} The highest level of data that traverses the **[Organization 2] [System 2 Name]** is Sensitive but Unclassified (SBU). This may include, but is not limited to, Sensitive Personally Identifiable Information, For Official Use Only, financial, and/or Law Enforcement Sensitive data.

4.5 Services Offered

{Describe the nature of the information services (e.g. E-mail, FTP, data base query, file query, general computational services, etc.) offered over the interconnected system by each participating organization.}

{Sample} The interconnection between the **[Organization 1] [System 1 Name]** and the **[Organization 2] [System 2 Name]** are supported by Multiprotocol Label Switching (MPLS) and Dynamic Multipoint Virtual Private Network (DMVPN) technologies. The **[Organization 1] [System 1 Name]** provides WAN connectivity services, Internet services, and perimeter security protection to the **[Organization 2] [System 2 Name]**.

Services and ports that are needed to access the Department systems are listed in Appendix A (Ports, Protocols and Services).

4.6 Period of Operation

{Specify the time period (Day, Month, Year) that the system will be available. Some ISAs may involve temporary set-up and tear-down under the 1 year window, e.g., FEMA after a natural disaster, Component to Vendor, etc. See the example provided below.}

{Sample} Both systems are operational 24 hours a day, 7 days a week.

4.7 User Community

{Enter a thorough explanation of the "user community" and/or "information recipients," including any formal access approvals, to be served by the interconnected systems to include their background check levels and nationality of the defined user communities, in particular the lowest background check level of any individual who shall have access to the interconnected system. If there is no user community defined, this should be documented.}

{Sample} The user community is comprised of **[Organization 1]** and **[Organization 2]** contract and employees. Additionally, other users may include employees or contract employees of other DHS Components and other Federal agencies. All users of both systems will have appropriately adjudicated suitability background investigations and will be US citizens. If non-US citizen have

access to either system, appropriate exceptions will be documented in accordance with DHS Policy.

Under normal conditions, only U.S. Citizens are allowed access to DHS systems and networks, however, at times there is a need to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to appropriate policies are treated separately from standard exceptions and waivers. The approval chain for an exception to the U.S. Citizenship requirement flows through the Component Head, the Office of Security, and the Chief Information Officer. Attachment XX to the DHS 4300A, "*Information Technology Security Program, Sensitive Systems*" provides an electronic form for requesting exceptions to the U.S. Citizenship requirement.

4.8 Information Exchange Security

{Enter a description of all system security technical services pertinent to the secure exchange of information/data among and between the systems in question.}

{Sample} Information exchange will be encrypted using FIPS 140 validated encryption as the federal required encryption standard. Dynamic Multipoint Virtual Private Network (DMVPN) provides a mechanism for the dynamic negotiation of IPSec encrypted tunnels between any two endpoints, alleviating the need for complex router configurations.

{Sample} **[Organization 1]** maintains the following IDS/IPS and firewalls on the **[Organization 1] [System 1 Name]**:

- IDS/IPD: **[_____]**
- Data Firewalls: **[_____]**

{Sample} **[Organization 2]** maintains the following IDS/IPS and firewalls on the **[Organization 2] [System 2 Name]**:

- IDS/IPD: **[_____]**
- Data Firewalls: **[_____]**

{Sample} Both organizations will ensure that virus and spyware detection and eradication capabilities are used where appropriate (e.g., workstations, laptops, servers, etc.) and that adequate system access controls are in place and maintained on all components connected to the systems.

{Sample} Specific protocols and ports that are needed to support this interconnection are provided in attachment A: Ports and protocols not specifically defined in Attachment A will be approved by DHS firewall change control procedures.

4.9 Trusted Behavior / Rules of Behavior

{Summarize the aspects of trusted behavior that are expected by and from each system in the interconnection. For example, each system is expected to protect the information belonging to the other through the implementation of a security program(s) that provide(s) for defense against intrusion, tampering, viruses, etc. In other words those things expected (not guaranteed) by each

system to further enhance the security posture and if those items have operational capabilities. Do not enter statements of Law or policy; those are typically in the MOU covering the concept.}

{Sample} The **[Organization 1] [System 1 Name]** users and **[Organization 2] [System 2 Name]** users, to include system administrators, are expected to protect data in accordance with the policies, standards, and regulations specified for each system. This includes **[Organization 1]** and **[Organization 2]** policy and the documented rules of behavior for each system. The following documents specify specific rules of behavior for each system:

{Sample} **[Organization 1 & 2]**: Rules Of Behavior

{Sample} **[Organization1 & 2]**: Information Systems Rules of Behavior and User Agreement

4.10 Formal Security Policy

{Enter the titles and dates of the formal security policies that govern each system.}

{Sample} Policy documents that govern the protection of the data between the two organizations systems are: **[Organization 1's] [Policy Name] [Policy Date] and [Organization 2's [Policy Name] [Policy Date].**

4.11 Incident Reporting

{Describe the agreements made concerning the reporting of and responses to information security incidents for both organizations. For example, "Each organization will report incidents in accordance to their own (procedure name) procedures." If no Incident Reporting is being performed, this should be documented.}

{Sample} The organization discovering a security incident will report it in accordance with the organization's incident reporting procedures and ensure that the other connecting organization is notified. **[Organization 2]** shall report security incidents to the DHS Security Operations Center (SOC). DHS SOC contact information is:

DHS OneNET Support: 1-877-DHS1NET or 1-877-347-1638
Option 1 = NOC
Option 2 = SOC

DHS SOC Direct Line: (703) 921-6505

[Organization 1] [System 1 Name] personnel will be notified of any security incident that may have an operational or security impact on the **System 1** resources. Likewise, the **[Organization 2]** SOC shall be notified of any security incident that may have an operational or security impact on **[System 2 Name]** connected to the **[Organization 1] [System 1 Name]**.

4.12 System Monitoring

{Identify availability, performance, and activity monitoring tools (e.g., WUG, OpenView, ISS Server Sensor, Nagios, FogLight, BlackIce, Axent ITA,), monitoring protocols (ICMP, SNMP), and monitoring/alerting consoles used by each organization.}

{Sample} The **[Organization 1] [System 1 Name]** performance and operations are monitored and managed using the following products and tools:

List the tools

{Sample} **[Organization 1] [System 1 Name]** is deploying and/or using the following products and capabilities to monitor security vulnerabilities and compliance:

List the tools

{Sample} The **[Organization 2] [System 1 Name]** performance and operations are monitored and managed using the following products and tools:

List the tools

{Sample} **[Organization 2] [System 1 Name]** is deploying and/or using the following products and capabilities to monitor security vulnerabilities and compliance:

List the tools

4.13 Security Audit Trail Responsibility

{Enter a description of how the audit trail responsibility is to be handled and what events each shall log. Describe the security officer role and include specifics concerning what an ISSO can do and which files would be given (ownership) to this role, if no audit trail is being performed, this should be documented.}

{Sample} Both parties are responsible for auditing system security events and user activities involving the interconnection. Activities that will be recorded include:

- Event type
- Date and time of event
- User identification
- Workstation/server identification
- Success or failure of access attempts
- Security actions taken by system administrators or ISSOs.

Audit logs will be retained for 90 days on-line and available for at least one (1) year (as long as the entries do not contain PII).

4.14 Specific Equipment/Service Restrictions

{Describe any revised or new restriction(s) to be placed on terminals, including their usage, location, and physical accessibility. Add any specific restrictions on either system.}

{Sample} The use of specific prohibited or restricted services, protocols, and ports listed in the DHS 4300A, "*Information Technology Security Program, Sensitive Systems*" require an approved waiver or exception agreement between the system AOs. Any additional interconnections to either system shall be documented in the appropriate security documentation and each party shall be notified of the new interconnections.

4.15 Dial-Up/Remote Connectivity

{Describe any special considerations for dial-up or remote connections) to either system in the proposed interconnection including additional security risks and any safeguards to mitigate them.}

{Sample} **[Organization 1]** currently uses a Cisco VPN for remote access to the **[Organization 1] [System 1 Name]**.

{Sample} **[Organization 2**] uses the **Organization 1**-managed Cisco VPN for remote **[Organization 2] [System 2 Name]** access.

4.16 Training and Awareness

{Enter the details of any new or additional security awareness, training requirements, and the assignment of responsibility for conducting it throughout the life cycle of the interconnected system.}

{Sample} Both parties will ensure that all individuals using the systems (i.e., **[Organization 1] [System 1 Name]** and **[Organization 2] [System 2 Name]**) have attended initial basic and annual refresher Computer Security Awareness and Training. Additionally, both parties will ensure that persons with significant security responsibilities for the systems receive annual role based training covering their specific areas of responsibility. This training should ensure that staff members know how to report suspicious or prohibited activities.

4.17 Security Documentation

{Enter the agreement to create and maintain security C&A documentation in accordance with each organization's System Development Life Cycle. Indicate whether the documentation is available to each party and who is responsible for providing the documentation.}

{Sample} The **[Organization 1] [System 1 Name]** and **[Organization 2] [System 2 Name]** Certification and Accreditation (C&A) documentation (e.g., System Security Plan, Contingency Plan, Risk Assessments and Security Assessments, Interconnection Security Agreements, etc.) and all other security related documents will be made available to each party for review and acceptance. SA documentation will be updated to reflect the establishment of this interconnection and whenever a significant system change occurs or at least annually. This ISA shall be updated should any of the information contained within change. The following information, at a minimum will be maintained accurate within this ISA:

- Names of interconnected systems
- Organizations owning the other systems
- Type of interconnection
- Name and title of authorizing management officials (e.g. Chief Information Officer or Designated Authorizing Authority)
- Interaction among the systems
- Hardware inventory

- Software inventory
- Rules of Behavior

{Sample} All future changes relating to the security architecture of either system will be updated within the corresponding security documents. The assigned Information System Security Officer(s) for each system shall provide the security documentation to the each organization upon request.

4.18 Change Control

{Define the formal process used to change any architecture component, process, or agreement. See the example provided below.}

{Sample} Significant changes to the system architecture, documentation, or configurations will be reviewed, approved and documented in accordance with each organization's configuration/change control process. Each organization shall notify the other if a system change significantly changes the approved security posture of the system or introduces new significant residual risk to either system. Whenever significant changes are made at one or both organizations, e.g., through additional staff, service, etc., this should be recorded as an addendum to the original ISA.

5.0 TOPOLOGICAL DRAWING

{All communications paths, circuits, etc. used for the interconnection beginning with the Customer-owned system(s) traversing through all interconnected systems to the non-Customer end-point. The drawing should depict the logical location of all components. (e.g., Mainframe Computers, Host Processors, Hubs, Firewalls, Encryption Devices, Routers, Frame Relay Devices, Secure Frame Units (SFU), Communications Service Units (CSU), Data Service Units (DSU), Customer Personal Computers, etc.)]. Recommend placing the drawing in an appendix so the drawing can be easily updated when needed without impacting the primary document.

The point of demarcation should be clearly identified at each end of the circuit. Note: Any sensitive information such as IP Addressing schemas should not be included in these drawings. The ISSO for each Component ISA should have the appropriate facility to house the detailed version of these supporting documents if needed for review or audit.}

*{Sample}*An architecture diagram showing the system interconnection is contained in Attachment B. The diagrams shall illustrate all communication paths, circuits, and other components used for the interconnection.

6.0 SIGNATORY AUTHORITY

{Sample} This ISA is valid for three (3) years after the latest date on either signature listed below, if the technology documented herein does not change or if there are no other intervening requirements for updates. At that time it must be reviewed, updated, and reauthorized. The security controls for this interconnection will be reviewed at least annually or whenever a significant change occurs. Either party may terminate this agreement with thirty days advanced notice. Noncompliance on the part of either organization or its users or contractors with regards to security policies, standards, and procedures explained herein may result in the immediate termination of this agreement.

7.0 SIGNATURES

[Organization 1] [System 1 Name] AO Name	
Signature & Date	
[Organization 2] [System 2 Name] AO Name	
Signature & Date	

Attachment A:

{Sample} **[Organization 1]** and **[Organization 2]** Allowed Ports, Protocols & Services

The following ports, protocols, and services are allowed between **[Organization 1]** and **[Organization 2]** Security Domains by default.

{ADD ports and services}

Ports, Protocols, and Services Chart (Example)		
	[Organization 1]	**[Organization 2]**
Port Number (Server / Destination	*{Sample}* 443	*{Sample}* 443
IP Protocol (TCP/UDP)	*{Sample}* TCP	{Sample} TCP
Software Application	*{Sample}* Apache	*{Sample}* Apache
Data Type / Purpose	*{Sample}* Remote Administration	*{Sample}* Remote Administration
PII Data?	No	No
Financial Data?	No	No
Encryption used	*{Sample}* SSL	

Attachment B:

[Organization 1] [System 1 Name] to **[Organization 2] [System 2 Name]** Interconnection Architecture Diagram

{Note: Any sensitive information such as IP Addressing schemas should not be included in these drawings. The ISSO for each Component ISA should have the appropriate facility to house the detailed version of these supporting documents if needed for review or audit.}

{Add Diagrams as Needed}