U.S. Customs and Border Protection

Attachment N

Preparation of Interconnection Security Agreements

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release based solely on DHS 4300A, Version 6.1.1, attachment. There are no substantive differences between this CBP attachment and its source DHS attachment. This attachment is included as part of the CBP 1400-05D handbook suite to enable the CBP user to be able to access all IT security policies (DHS as well as CBP specific) at one location.
2.0	December 21, 2010	No Changes.

CONTENTS

1.0 PURPOSE

This document provides CBP with information on the creation and use of Interconnection Security Agreements (ISAs). ISAs are vital in protecting 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*, August 2002. An ISA is required whenever the security policies of the interconnected systems are not identical and the systems are not administered by the same entity/Designated Accrediting Authority (DAA). The ISA documents the security protections that must operate on interconnected systems to ensure that transmissions between systems permit only acceptable transactions. The 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.

The ISA must be reissued whenever a significant change occurs to any of the interconnected systems. The designated ISSO must review the ISA related to their respective system as part of their annual FISMA self-assessment. ISAs need not be reissued unless a significant system change has occurred or three years have elapsed since issuance.

2.0 BACKGROUND

This document is supported by the IT Security Policy on network connectivity in the *CBP 1400-05D, IT Security Policy and Procedures Handbook* that sets forth the technical and management controls necessary to secure network connectivity. This attachment is directly related and consistent with the DHS 4300A, Version 6.1.1, Attachment N.

More detailed interconnection guidance is provided by NIST Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002. SP 800-47 is the basis for ISA treatment in all three CBP documents. NIST has also issued a condensed summary of the SP 800-47 material in an Information Technology Laboratory (ITL) Bulletin, *Secure Interconnections for Information Technology Systems*, February 2003.

3.0 SCOPE

This attachment expands on the interconnection material in contained in the 1400-05D policy handbook in the following areas:

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

Attachment N applies to all CBP systems.

4.0 REFERENCES

- CBP 1400-05D, IT Security Policy and Procedures Handbook

- CBP IT Security Policy Directive
- DHS Sensitive Systems Policy Directive 4300A
- DHS 4300A Sensitive Systems Handbook
- NIST, Security Guide for Interconnecting Information Technology Systems, SP 800-47, August 2002
- NIST, Secure Interconnections for Information Technology Systems, ITL Bulletin, February 2003

5.0 POLICY

The applicable network connectivity policy statements from *CBP 1400-05D* are the following:

DHS Policy
a. Components shall ensure appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component.
b. Interconnections between sensitive IT systems and IT systems not controlled by the DHS shall be established only through controlled interfaces. The controlled interfaces shall be accredited at the highest security level of information on the network.
c. Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the official designated by the DAA to have signatory authority.
d. ISAs shall be reissued every three years or whenever any significant changes have been made to any of the interconnected systems.
e. ISAs shall be reviewed as a part of the annual FISMA self-assessment.

6.0 PROCEDURES

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. SP 800-47 should be consulted for details, along with other guidelines and related DHS policy and Handbook sections applicable to specific steps.

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 Attachment N.
- Establishing: Includes steps involving detailed technical preparations, culminating in a SIIP. (Although the SIIP comes after the ISA, Appendix N3 of this document includes a brief outline of the SIIP, because 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 beyond the scope of Attachment N.

- Disconnecting: Includes processes for planned and emergency disconnections and for restoring a connection. This material is beyond the scope of Attachment N.

6.1 Steps in Planning an Interconnection

The planning steps required and their key components are the following:

Step 1. Establish joint planning team:

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

Step 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.

Step 3. Perform certification and accreditation (C&A):

- Perform C&A for the individual systems, or confirm that they are currently accredited.
- For systems requiring a new or updated C&A, develop required technical products in compliance with C&A guidance: system security plan, risk assessment, contingency plan, security review.

Step 4. Determine interconnection requirements:

- Conduct analysis required for ISA and MOU/A development (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

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

- Segregation of duties
- Incident reporting and response
- Contingency planning
- Data element naming and ownership
- Data backup
- Change management
- Rules of behavior
- Security training and awareness
- Roles and responsibilities
- Scheduling
- Costs and budgeting

Step 5. Document interconnection agreement:

- Produce the ISA and MOU/A.
- Establish access controls for sensitive ISAs and MOU/As.

Step 6. Approve or reject interconnection:

- ISSO and the CA reviews the draft version of the ISA, MOU/A, and the CA determines the approval of the ISA.
- DAAs (or officials designated by the DAAs) review ISA, MOU/A, and other relevant documentation, including the SIIP[2].
- Distribute copies of approved documents to responsible officials.
- For an interim approval to operate, the DAA must 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 SP 800-47 are the following[3]:

Step 1. Develop a SIIP

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

[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 SP 800-47 provides useful discussion of these steps.

Step 2. Execute the implementation plan

- Implement or configure security controls in accordance with the SIIP. The brief discussions in 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 system security plans.
- Perform recertification and re-accreditation.

Step 3. Establish the interconnection

7.0 RESPONSIBILITIES

The personnel responsibilities defined are the following:

Person Responsible	Task
CISO	• 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/systems periodically to ascertain if changes have occurred that could adversely affect security.
DAA	• 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.
Certifying Agent	• Review the Interconnection Security Agreement to ensure that all relevant security controls are in place.
Network Administrators	• Ensure technical controls governing use of the external connection remain in place and function properly. • Assist in development of the ISA.

[4] The list of topics in Appendix C of 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
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 System Security Plan, Risk Assessment, and security operating procedures. • Review ISAs as a part of the annual FISMA self-assessment. • Monitor compliance. • Research and ensure that the any necessary MOUs are in place relevant to the ISA being developed. MOUs are managed through the Office of Rules and Regulations (ORR).
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

Interconnection Security Agreement

An Interconnection Security Agreement (ISA) describes a connection in sufficient detail to serve as a sound basis for approving a system-to-system connection. The protection for the connected systems is meant to equal or exceed their individual protection. The signing of an ISA by the DAA is a prerequisite to operating the associated connection.

An ISA supports a separate MOU/A, which defines the general responsibilities for establishing, operating and securing a connection. (Appendix N2 describes MOU/As.) An ISA should refer to its associated MOU/A(s). SP 800-47 prescribes the addition of a reverse reference whenever an existing MOU/A is revised. ISAs that contain For Official Use Only (FOUO) or other restricted information shall be so labeled and protected in accordance with the applicable regulations of both organizations.

Figure N1-1 shows the ISA cover page format prescribed in SP 800-47. The following ISA outline is based on the description given in SP 800-47, Appendix A. The outline includes both standard and optional topics. It also allows tailoring of the ISA to cover additional security-relevant matters that are important to the signing organizations. Appendix A of SP 800-47 includes an ISA example. Appendix N4 of this document includes a template for an ISA.

FOR OFFICIAL USE ONLY

INTERCONNECTION SECURITY AGREEMENT

Between "Organization A"
and
"Organization B"

(ORGANIZATIONAL SEALS HERE)

SAMPLE

(DATE HERE)

(Organization A) **(Organization B)**

(Relevant Organization)

(Organizationally Assigned Unique Tracking Number)

FOR OFFICIAL USE ONLY

Figure N1-1. ISA Title Page Sample

Section 1: Interconnection Statement of Requirements

- Identity of the participating organizations and any higher-level agency responsible for the initiative.
- Identity of systems to be connected.
- Reference any MOU/A(s) and identify primary points of contact for each system
- Provide a brief statement of the requirements for the interconnection, including the derived benefits.

Section 2: System Security Considerations

Standard Topics (from SP 800-47):

- 2.1 General Information/Data Description. Describe the information and data that will be made available, exchanged, or passed one-way-only by the interconnection of the two systems.
- 2.2 Services Offered. Describe the nature of the information services (e.g., e-mail, file transfer protocol [FTP], database query, file query, general computational services) offered over the interconnection by each organization.
- 2.3 Data Sensitivity. Enter the sensitivity level of the information that will be handled through the interconnection, including the highest level of sensitivity involved (e.g., Privacy Act, Trade Secret Act, Law Enforcement Sensitive, Sensitive-But-Unclassified) and the most restrictive protection measures required.
- 2.4 User Community. Describe the user community that will be served by the interconnection, including their approved access levels and the lowest approval level of any individual who will have access to the interconnection. Also, discuss requirements for background investigations and security clearances, if appropriate.
- 2.5 Information Exchange Security. Describe all system security technical services (e.g., encryption, controlled access facilities, authentication) pertinent to the secure exchange of data between the connected systems.
- 2.6 Rules of Behavior. Summarize the aspects of behavior expected from users who will have access to the interconnection. Each system is expected to protect information belonging to the other through the implementation of security controls that protect against intrusion, tampering, and viruses, among others. Do not enter statements of law or policy. Such statements typically are addressed in the MOU/A.
- 2.7 Formal Security Policy. Enter the titles and dates of the formal security policies that govern each system.
- 2.8 Incident Reporting. Describe the agreements made regarding the reporting of and response to information security incidents for both organizations. For example, “Each organization will report incidents in accordance with its own (procedure name) procedures.”
- 2.9 Audit Trail Responsibilities. Describe how the audit trail responsibility will be shared by the organizations and what events each organization will log. Specify the length of time that audit logs will be retained. If no audit trail is performed, so state.

Optional Topics (from SP 800-47, depending on need):

- Security Parameters. Specify the security parameters exchanged between systems to authenticate that the requesting system is the legitimate system and that the class(es) of service requested is approved by the ISA. For example, at the system level, if a new service such as e-mail is requested without prior coordination, it should be detected, refused, and documented as a possible intrusion until the interconnected service is authorized. Also, additional security parameters may be required (e.g., personal accountability) to allow the respondent system to determine whether a requestor is authorized to receive the information and/or services requested and whether all details of the transaction fall within the scope of user services authorized in the ISA.
- Operational Security Mode. If both parties use the concept of Protection Levels and Levels-of-Concern for Confidentiality, Integrity, and Availability based on their implementation common criteria, enter the values for each as documented for both systems. Optionally, the security mode of operations could be documented for both systems.
- Training and Awareness. Enter the details of any new or additional security training and awareness requirements, and the assignment of responsibility for conducting training and awareness throughout the life cycle of the interconnection.
- Specific Equipment Restrictions. Describe any revised or new restriction(s) to be placed on terminals, including their usage, location, and physical accessibility.
- Dialup and Broadband Connectivity. Describe any special considerations for dialup and broadband connections to any system in the proposed interconnection, including security risks and safeguards used to mitigate those risks. See National Institute of Standards and Technology (NIST) Special Publication 800-46, *Security Guide for Telecommuting and Broadband Communications*, for more information.
- Security Documentation. Enter the title and general details of each organization's system security plan, including the assignment of responsibilities for developing and accepting the plan, as well as any other relevant documentation.

Additional Topics:

Additional topics are determined by the DAAs, based on particular needs associated with the planned connection.

Section 3: Topological Drawing

This section consists of one or more figures depicting:

- The identity and locations of the systems and all components involved in their interconnection (e.g., firewalls, routers, switches, hubs, servers, encryption devices, workstations)
- Representation of all communications paths and types of connection (e.g., frame relay, T1)

Section 4: Signatory Authority

- Signature and date of signature for the DAA or other designated official for each organization

- Date of ISA expiration (should agree with the MOU/A expiration date)
- Requirements for periodic or condition-based review of the ISA
- Other statements, if any, required by the DAA (e.g., conditions and procedure for terminating or extending the agreement)

Appendix N2

Memorandum of Understanding/Agreement

A Memorandum of Understanding/Agreement (MOU/A) 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. SP 800-47 allows use of organization-specific MOU/A formats but provides an example, based on the following outline:

Section 1: Supersession

Identify documents, if any, superseded by this MOU/A.

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/A 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 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/A 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 N3

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/A and ISA, agreements with more administrative than technical content. 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/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 N4

Interconnection Security Agreement Template