5 FAH-11 H-820
ESTABLISHING CONNECTIVITY

(CT:IAH-2; 03-12-2007)
(Office of Origin: IRM/IA)

5 FAH-11 H-821 CONNECTIVITY

(CT:IAH-2; 03-12-2007)

a. National policy guidance requires agencies to protect interconnections when sharing information with other entities. The Department must establish formal agreements to have interconnections with non-Department entities. OMB Circular A-130, Appendix III, as supplemented by the National Institute Standards and Technology (NIST) Special Publication (SP) 800-47 and Committee for National Security Systems (CNSS) policies and instructions, requires agencies to obtain written management authorization before connecting their information technology (IT) systems to other systems based on an acceptable level of risk. The written authorization should define the rules of behavior for individual users of each system, along with the controls that must be maintained for the system interconnection. The system security plans of the connecting parties should include these rules.

b. Through interconnection agreements, the Department may connect to several types of governing entities, including other national governments, other Federal agencies, contractors, state and local governments, non-government organizations, etc.

c. With regard to interconnection agreements that are international agreements, Department policy requires the Office of Legal Adviser (L) to ensure that international agreements are properly drafted, and that the agreed policy is expressed clearly and fully in the text of the agreement. (See 11 FAM 730 for details on international agreements.)

5 FAH-11 H-822 CONNECTION PLANNING

(CT:IAH-2; 03-12-2007)

The purpose of the planning phase is to ensure that the proposed interconnection will operate as efficiently and securely as possible. During this phase, the participating parties perform preliminary activities and examine all relevant technical, security, and administrative issues related to the agreement. The recommended steps to facilitate the planning process

are in 5 FAH-11 H-822.1 through H-822.6.

5 FAH-11 H-822.1 Establish Planning Team

(CT:IAH-2; 03-12-2007)

A joint planning team composed of appropriate managerial and technical staff to promote regular communication between the parties throughout the life cycle of the interconnection should be established. This team is responsible for coordinating all aspects of the planning process and ensuring that the interconnection process has clear direction and sufficient resources.

5 FAH-11 H-822.2 Define the Business Case

(CT:IAH-2; 03-12-2007)

Both parties (or the joint planning team) should work together to define the purpose of the interconnection, determine how it will support their respective mission requirements, and identify potential costs and risks in implementing and maintaining the interconnection. Defining the business case will establish the basis for the interconnection and facilitate the planning process.

5 FAH-11 H-822.3 Perform Certification and Accreditation

(CT:IAH-2; 03-12-2007)

Before interconnecting their information systems, each party must ensure that its respective system is properly certified and accredited (C&A) in accordance with mutually acceptable guidelines. Department and other Federal agency systems must be certified and accredited in accordance with 5 FAM 1065.3 and 1065.4.

5 FAH-11 H-822.4 Determine Requirements

(CT:IAH-2; 03-12-2007)

a. The parties (or the joint planning team) should identify and examine all relevant technical, security, and administrative issues surrounding the proposed interconnection. The parties should use this relevant information to develop an Interconnection Security Agreement (ISA) and a Memorandum of Understanding or Agreement (MOU/MOA) or, if preferable, an overall agreement that combines an ISA and MOU/MOA. For connection that involves a contractual relationship, the information must be documented in a Form DD-254, Department of Defense Contract Security Classification Specification. (**NOTE**: The Department uses this

Department of Defense (DoD) DD-254 form.) The ISA and MOU/MOA, or Form DD-254, must include language that addresses or covers the following issues:

(1) The level and method of interconnection;

(2) The impact on existing infrastructure and operations;

(3) Hardware requirements to support the interconnection;

(4) Software requirements, including licensing requirements (see 5 FAM 915.11-1), to support the interconnection;

(5) Sensitivity of the data to be available, exchanged, or passed;

(6) User access rights that correspond to data sensitivity levels;

(7) Services and applications to be provided under the agreement;

(8) Mode of operation for classified and unclassified systems;

(9) Security controls to be implemented;

(10) Segregation of duty requirements for certain functions;

(11) Privacy policies and procedures, including the safeguarding of personally identifiable information;

(12) Incident reporting and response requirements, including procedures for responding to unauthorized disclosures of or access to personally identifiable information;

(13) Contingency planning;

(14) Data element naming and ownership;

(15) Data backups;

(16) Management of configuration changes;

(17) User security clearances;

(18) User rules of behavior;

(19) Security training (to include foreign disclosure training) and awareness;

(20) Roles and responsibilities;

(21) Scheduling for all activities involved in planning, establishing, and maintaining the interconnection;

(22) Identifying and budgeting for the costs to plan, establish, and maintain the interconnection through Department budget and IT Capital Planning processes; and

(23) Resolving conflicts between the parties.

b. Guides to developing ISAs and MOUs/MOAs, which are recommended by

NIST, are set forth in 5 FAH-11 Exhibits H-822.4(1)(A) and H-822.4(2)(A). Examples of possible ISAs and MOU/MOAs, which are recommended by NIST, are set forth in 5 FAH-11 Exhibit H-822.4(1)(B) and H-822.4(2)(B).

5 FAH-11 H-822.5 Document Agreement

(CT:IAH-2; 03-12-2007)

a. The parties must maintain a formal agreement, signed by the Designated Approving Authorities (DAAs) or other authorizing management officials, governing the interconnection and the terms the parties must follow. The formal documents the Department must develop and retain are:

   (1) An ISA and an MOU/MOA;

   (2) If the Department and another national government or another national agency are involved, an international agreement, which may be either in addition to an ISA and an MOU/MOA, or may incorporate the elements of an ISA and an MOU/MOA; and

   (3) If a contractual relationship exists with the organization connecting to the Department, then a Form DD-254 must be used instead of an ISA and an MOU/MOA.

b. The Office of the Legal Adviser must clear all draft international agreements. (See 11 FAM 730.)

c. An ISA documents the requirements for connecting the IT systems, describes the security controls that will be used to protect the systems and data, contains a topological drawing for the interconnection, and provides a signature line.

d. An MOU/MOA documents the terms and conditions for sharing data and information resources. The MOU/MOA defines the purpose of the interconnection; identifies relevant authorities; specifies the responsibilities of both parties; and defines the terms of agreement, including apportionment of cost, and the timeline for terminating or reauthorizing the interconnection.

e. The Department uses a Form DD-254 to document all the information normally contained in the ISA and MOU/MOA, and incorporates this required information into the contract.

5 FAH-11 H-822.6 Approve/Deny System Interconnection

(CT:IAH-2; 03-12-2007)

The team or parties must submit the ISA and MOU/MOA (including

international agreements that incorporate them) or Form DD-254 to the Designated Approving Authority (DAA) or other authorizing management official of each party, requesting formal authorization for the interconnection. Each DAA or authorized management official must authorize, in writing, the MOU/MOA and ISA or Form DD-254 before establishing an interconnection.

5 FAH-11 H-823 CONNECTION IMPLEMENTATION

(CT:IAH-2; 03-12-2007)

To ensure that the IT systems are connected properly and securely, the parties (or the joint planning team) must develop a System Interconnection Implementation Plan. The purpose of the plan is to centralize all aspects of the interconnection effort in one document and to clarify how the ISA will be implemented. (See 5 FAH-11 Exhibit H-823.)

5 FAH-11 H-823.1 Develop Implementation Plan

(CT:IAH-2; 03-12-2007)

The implementation plan for the interconnection must:

(1) Describe the information systems to be connected;

(2) Identify the sensitivity or classification level of the data that will be made available, exchanged, or passed only one-way across the interconnections;

(3) Identify personnel who will establish and maintain the interconnection, and specify their responsibilities and security clearances;

(4) Identify implementation tasks and responsibilities;

(5) Identify and describe security controls that will be used to protect the interconnected systems and data;

(6) Provide test procedures and measurement criteria to ensure that the interconnection operates properly and securely;

(7) Specify training requirements for users, including training schedules and foreign disclosure requirements;

(8) Include cost and resources requirements and required dates of operation; and

(9) Cite or include all relevant documentation, such as systems security plans, contingency plans, design specifications, and standard operating procedures.

5 FAH-11 H-823.2 Execute Implementation Plan

(CT:IAH-2; 03-12-2007)

The senior members of the planning team must review and approve the plan before implementation. It must then be executed through the following tasks:

(1) Implementing or configuring the security controls, including:

(a) Installing new firewalls or reconfiguring existing firewalls;

(b) Implementing intrusion detection systems;

(c) Installing or configuring devices to record activities across the interconnection;

(d) Implementing mechanisms to identify and authenticate users;

(e) Utilizing access control lists and access rules to specify access privileges of authorized personnel;

(f) Installing anti-virus software on all servers and workstations linked to the interconnection;

(g) Using encryption to ensure data cannot be read by unauthorized users; and

(h) Placing hardware and software supporting the interconnection, including the interconnection points, into a secure location that is protected from unauthorized access, interference, or damage;

(2) Installing or configuring new hardware and software including:

(a) Installing communication lines;

(b) Installing virtual private network (VPN) software on servers and local workstations;

(c) Installing routers or switches to connect to the communication lines between the system or configuring existing devices;

(d) Installing hubs to join multiple computers into a single network segment, if required;

(e) Installing appropriate servers to support services provided across the interconnection, such as databases and application servers; and

(f) Configuring workstations by providing a menu option or a link to enable authorized users to invoke the interconnection;

(3) Integrating applications or protocols for services that are provided across the interconnection. Examples include word processing,

database applications, e-mail, web browsers, application servers, authentication severs, domain servers, editing programs, and communication programs;

(4) Conducting operational and security testing to ensure equipment operates properly and to identify ways for unauthorized users to circumvent or defeat security controls. Determining whether or not the test results meet a mutually agreed level of acceptable risk and whether or not other actions are required;

(5) Conducting security and awareness training for all authorized personnel who will be involved in managing, using, and/or operating the interconnection;

(6) Using systems security plans and related documents to reflect the changed security environment in which each party's systems now operate. NIST recommends the security plans include the following information on the system interconnection:

(a) Names of interconnected systems;

(b) Party owning the other system;

(c) Type of interconnection;

(d) Short discussion of major concerns or considerations in determining the interconnection;

(e) Names and titles of management officials authorizing the interconnection;

(f) Date of authorization;

(g) System of record, if applicable (Privacy Act data);

(h) Sensitivity level of each system;

(i) Interaction among systems;

(j) Hardware inventory;

(k) Software inventory;

(l) Security concerns; and

(m) Rules of behavior governing the interconnections;

(7) Performing periodic recertification and re-accreditation of each party's respective system to verify that security controls remain acceptable; and

(8) Activating the interconnection for use by both parties following prescribed guidelines. NIST recommends that both parties also closely monitor the interconnection for at least three months to ensure that it operates properly and securely.

5 FAH-11 H-824 MAINTAIN CONNECTION

(CT:IAH-2; 03-12-2007)

After establishing the interconnection, it must be actively maintained to ensure that it operates properly and securely. The recommended activities include the following.

(1) **Maintaining clear lines of communication**. Both parties should maintain clear lines of communication and communicate regularly.

(2) **Maintaining equipment**. The parties should agree on who will maintain the equipment used to operate the interconnection.

(3) **Managing user profiles**. Both parties should actively manage user profiles to preclude inappropriate access to data or information.

(4) **Conducting security reviews**. Both parties should review the interconnection's security controls at least annually, and whenever a significant change (as defined in the agreement) to the interconnection or the party's system occurs, to ensure that they are operating properly.

(5) **Analyzing audit logs**. One or both parties should analyze audit logs at predetermined intervals to detect and track unusual or suspicious activities across the interconnection.

(6) **Reporting and responding to security incidents**. Both parties should notify each other of intrusions, attacks or internal misuse, so the party can take steps to determine whether or not its system has been compromised.

(7) **Coordinating contingency planning activities**. Both parties should coordinate the planning, training, testing, and exercising of contingency plans to minimize the impact of disasters and other contingencies that could damage the connected systems or jeopardize the confidentiality and integrity of shared data.

(8) **Performing change management**. Each party should establish a change control board or a similar body to review and approve planned changes to its respective system.

(9) **Maintaining system security plans**. Both parties should update their system security plans and other relevant documentation at least annually, and whenever there is a significant change (as defined in the agreement) to their systems or the interconnection.

5 FAH-11 H-825 DISCONNECT/RESTORE INTERCONNECTION

(CT:IAH-2; 03-12-2007)

To avoid disrupting the other party's IT system, a party should terminate, if possible, the interconnection in a methodical manner.

5 FAH-11 H-825.1 Planned Disconnection

(CT:IAH-2; 03-12-2007)

Before terminating the interconnection, the initiating party must notify the other party, in writing, and the other party should return an acknowledgement to the initiating party. The notification must describe the reason for the disconnection, provide the proposed timeline for the connection, and identify the technical and management staff that will conduct the disconnection.

5 FAH-11 H-825.2 Emergency Disconnection

(CT:IAH-2; 03-12-2007)

The ISA or Form DD-254 should address an emergency disconnection or termination. One or both parties may elect to abruptly terminate the interconnection during an emergency without providing written notification to the other party. A party should only take this extraordinary measure in extreme circumstances (e.g., during an attack, intrusion attempt or other contingency that exploits or jeopardizes the connected systems or their data). The decision to terminate should be taken only after consultation with appropriate technical staff and senior management.

5 FAH-11 H-825.3 Restore Interconnection

(CT:IAH-2; 03-12-2007)

The decision to restore the interconnection should be based on the cause and duration of the disconnection as follows:

(1) If the disconnection was due to an attack, intrusion or other contingency, then both parties must implement appropriate countermeasures to prevent a recurrence of the problem; or

(2) If the interconnection has been terminated for more than 90 days, then each party must perform a risk assessment on its respective system, and reexamine all relevant planning and implementation issues.

5 FAH-11 H-826 THROUGH H-829 UNASSIGNED

5 FAH-11 EXHIBIT H-822.4(1)A INTERCONNECTION SECURITY AGREEMENT (GUIDE)

(CT:IAH-2; 03-12-2007)

The Interconnection Security Agreement (ISA) documents the technical requirements of an interconnection between the parties. The ISA also supports the Memorandum of Understanding or Agreement (MOU/MOA) between the parties. An ISA development guide is provided below and a sample ISA is depicted in 5 FAH-11 Exhibit H-822.4(1)B.

Purpose of the ISA

The intent of the ISA is to document and formalize the interconnection arrangement between the parties and to specify any details that may be required to provide any overall security safeguards for the systems being interconnected. Under a valid ISA, a system with an approved interconnection with another party's system should meet the protection requirements equal to or greater than those implemented by the other party's system.

References

The authority for interconnectivity between IT systems is based on Office of Management and Budget Circular A-130 and a signed MOU/MOA between the two parties establishing the interconnection.

Scope

These guidelines are effective in the following system development life cycle (SDLC) phases noted with the checkmark.

CONCEPTS DEVELOPMENT		DEPLOYMENT	√
DESIGN		OPERATIONS	√
DEVELOPMENT	√	DISPOSAL	√

Procedure

An ISA is used to support an MOU/MOA that establishes the requirements for data exchange between two parties. The ISA is a distinct security-related document that outlines the technical solution and security requirements for the interconnection. It does not replace an MOU/MOA. Only the two Designated Approval Authorities (DAA) (or other authorizing management officials) whose names appear in Section 4 of the agreement (see below) should sign and authorize the ISA. The ISA should be formally signed before declaring the interconnection operational.

Contents of an Interconnection Security Agreement

The ISA should contain four sections addressing the need for the interconnection and the security controls required to protect the confidentiality, integrity, and availability of the systems and data. The extent of the information should be sufficient for the two DAAs to make a prudent decision about approving the interconnection. The four sections are as follows:

(1) Interconnection Statement of Requirements;

(2) Systems Security Considerations;

(3) Topological Drawing; and

(4) Signatory Authority.

Section 1: Interconnection Statement of Requirements

This section is used to document the formal requirements for connecting the two systems. The information presented should include the following:

(1) The requirement for the interconnection, including the benefits derived from having this interconnection;

(2) The names of the systems being interconnected; and

(3) The party and the name of the individual from that organization who requested the interconnection.

Section 2: System Security Requirements

a. Use this section to document the security features that are in place to protect the data and the systems being interconnected.

b. The following items should be addressed as required items in the ISA.

(1) **General Information/Data Description**. Describe the information or data that will be available, exchanged or passed only one-way.

(2) **Services Offered**. Describe the information services offered over the interconnection by each organization. These may include, but are not limited to, e-mail, file transfer protocol [FTP], database query, file query, and general computational services.

(3) **Data Sensitivity**. Describe the sensitivity level of the information that will be handled through the interconnection, including the highest level of sensitivity involved and the most restrictive protection measures required.

(4) **User Community**. Describe the user community, including their approved access levels and the lowest approval level of any individual who will have access to the interconnection. Also, address the requirements for background investigations and

security clearances.

(5) **Information Exchange Security**. Describe all system security technical services pertinent to the secure exchange of data between the connected systems.

(6) **Rules of Behavior**. Set forth the rules of behavior expected from users having access to the interconnection.

(7) **Formal Security Policy**. Document the formal security policies that govern the interconnection.

(8) **Incident Reporting**. Describe agreements made regarding the reporting of and response to information security incidents.

(9) **Audit Trail Responsibilities**. Audit trail responsibilities should be shared by the organizations and agreement made as to what events each organization will log. This section should describe these responsibilities.

(10) **Privacy Considerations**. Both parties should safeguard any personally identifiable information belonging to the U.S. Government and take measures to prevent any breach of its security.

c. The following items should be addressed in the ISA with a statement by the technical representative as to the applicability of the requirement for the ISA to be negotiated.

(1) **Security Parameters**. Provide a description of 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, if a new service (e.g., e-mail) is requested without prior coordination, it should be detected, refused, and documented as a possible intrusion until the interconnected service is authorized in the ISA.

(2) **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 (http://www.commoncriteriaportal.org/), enter the values for each as documented for both systems.

(3) **Training and awareness**. Enter the details of any new or additional security training and awareness requirements and the assignment of responsibility for conducting training awareness throughout the life cycle of the interconnection.

(4) **Specific Equipment Restrictions**. Describe any revised or new restrictions to be placed on terminals, including their usage, location, and physical accessibility.

(5) **Dial-up and Broadband Connectivity**. Describe any special considerations for dial-up and broadband connections to any system in the proposed interconnection, including security risks and safeguards used to mitigate those risks.

(6) **Documentation**. Enter the title and general details of each party's system security plan, including the assignment of responsibilities for developing and accepting the plan, as well as any other relevant documentation.

Section 3: Topological Drawing

The ISA should include a topological drawing illustrating the interconnectivity from one system to the other system (end-point to end-point). The drawing should include the following:

(1) A title page "SECTION 3: TOPOLOGICAL DRAWING";

(2) All communications paths, circuits, and other components used for the interconnection, from "Party A's system to Party B's system";

(3) The drawing should depict the logical location of all components (e.g. firewalls, routers, switches, hubs, servers, encryption devices, and computer work stations); and

(4) If required, mark the top and bottom of each page with an appropriate handling requirement (e.g., "SENSITIVE BUT UNCLASSIFIED" for agency to agency agreement).

Section 4: Signatory Authority

This section should include the following:

(1) The expiration date of the agreement;

(2) Periodic review requirements (e.g., date of the next review) and provisions for early termination;

(3) Other statements as required by the DAAs; and

(4) The signature of the DAA from each party and the date of the signatures.

5 FAH-1 H-822 EXHIBIT H-822.4(1)B INTERCONNECTION SECURITY AGREEMENT (ISA) SAMPLE

(CT:IAH-2; 03-12-2007)

SENSITIVE BUT UNCLASSIFIED

INTERCONNECTION SECURITY AGREEMENT

Between “Organization A”
and
“Organization B”

(ORGANIZATIONAL SEAL[S] HERE)

(DATE HERE)

(Organization A) (Organization B)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

INTERCONNECTION SECURITY AGREEMENT

SECTION 1: INTERCONNECTION STATEMENT OF REQUIREMENTS

The requirements for interconnection between “Organization A” and “Organization B” are for the express purpose of exchanging data between “System A,” owned by Organization A, and "System B,” owned by Organization B. Organization B requires the use of Organization A's "XYZ database" and Organization A requires the use of Organization B's "ABC database," as approved and directed by the Secretary of "Agency" in "Proclamation A," dated (date). The expected benefit is to expedite the processing of data associated with "Project R" within prescribed timelines.

SECTION 2: SYSTEM SECURITY CONSIDERATIONS

- General Information/Data Description. The interconnection between System A, owned by Organization A, and System B, owned by Organization B, is a two-way path. The purpose of the interconnection is to deliver the XYZ database to Organization B's Data Analysis Department and to deliver the ABC database to Organization A's Research Office.

- Services Offered. No user services are offered. This connection only exchanges data between Organization A's system and Organization B's system via a dedicated connection.

- Data Sensitivity. The sensitivity of data exchanged between Organization A and Organization B is Sensitive But Unclassified.

- User Community. All Organization A users with access to the data received from Organization B are U.S. citizens with a valid Organization A personnel security clearance. All Organization B users with access to the data received from Organization A are U.S. citizens with a valid Organization B personnel security clearance.

- Information Exchange Security. The security of the information being passed on this two-way connection is protected through the use of FIPS 140-2 approved encryption mechanisms. The connections at each end are located within controlled access facilities, guarded 24 hours a day. Individual users will not have access to the data except through their systems security software inherent to the operating system. All access is controlled by authentication methods to validate the approved users.

- Trusted Behavior Expectations. Organization A's system and users are expected to protect Organization B's ABC database, and Organization B's system and users are expected to protect Organization A's XYZ database, in accordance with the Privacy Act and Trade Secrets Act (18 U.S. Code 1905) and the Unauthorized Access Act (18 U.S. Code 2701 and 2710) and related authorities thereunder.

- Formal Security Policy. Policy documents that govern the protection of the data are Organization A's "XXX Policy" and Organization B's "YYY Policy."

- Incident Reporting. The party discovering a security incident will report it in accordance with its incident reporting procedures. In the case of Organization B, any security incident will be reported to Organization A within one hour, so that it may report the incident to the United States Computer Emergency Readiness Team (US-CERT). Policy governing the reporting of Security Incidents is set forth in 12 FAM 590 and 5 FAM 775a.

- Audit Trail Responsibilities. Both parties are responsible for auditing application processes and user activities involving the interconnection. Activities that will be recorded include 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. Audit logs will be retained for one (1) year and shared between the parties.

SECTION 3: TOPOLOGICAL DRAWING

(Insert a drawing here.)

SECTION 4: SIGNATORY AUTHORITY

This Interconnection Security Agreement (ISA) is valid for one (1) year from the last date included with either signature below. At the end of the one-year period, this agreement must be updated, reviewed, and reauthorized if an interconnection is to continue. Either party may terminate this agreement upon a 30-day advanced notice in writing or in the event of a security incident that necessitates an immediate response.

(Organization A Official)	(Organization B Official)
_____	_____
_____	_____
(Signature Date)	(Signature Date)

5 FAH-11 EXHIBIT H-822.4(2)A MEMORANDUM OF UNDERSTANDING/AGREEMENT (GUIDE)

(CT:IAH-2; 03-12-2007)

The agencies that own and operate the connected systems should establish a Memorandum of Understanding or Agreement (MOU/MOA) or an equivalent document that defines the responsibilities of both parties in establishing, operating, and securing the interconnection.

The MOU/MOA should include the following items:

1. Supersession

Identify any previous agreements that this memorandum supersedes.

2. Introduction

Describe the purpose of the memorandum, including identifying the parties and the IT systems involved.

3. Authorities

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

4. Background

Describe the IT system that will be connected, the data that will be shared, exchanged or passed only one-way across the interconnection, and the business purpose of the interconnection. The system description should include the formal name of the system, its functions, its physical location, its sensitivity or classification level, and the types of data it stores, processes, and /or transmits.

5. Communications

Discuss the communications that will be exchanged between the agencies throughout the duration of the interconnection.

6. Interconnection Security Agreement (ISA)

The parties should agree to develop and sign an ISA before the systems can be connected. In addition, describe the purpose of the ISA.

7. Security

Both parties must agree to abide by the security arrangements specified in the ISA. Similarly, both parties should certify that their respective system is

designed managed, and operated in compliance with all relevant international agreements, Federal laws, regulations, and policies.

8. Privacy Considerations

Both parties should adopt measures to protect personally identifiable information. Specific measures should include at least access safeguards, disclosure restrictions, marking and handling, and incident reporting procedures.

9. Cost Considerations

This section specifies who will pay for each part of the interconnection and the conditions for financial commitments. Typically, each party is responsible for the equipment necessary to interconnect its local system, whereas the agencies jointly fund the interconnection mechanism and media.

10. Timeline

Identify the expiration date for the agreement and procedures for reauthorizing it. In addition, stipulate that, with written notice to the other party, one party may terminate the memorandum.

11. Signatory Authority

The memorandum must include a signature line containing two signature blocks for each party's designated approval authority (DAA).

5 FAH-11 EXHIBIT H-822.4(2)B
MEMORANDUM OF UNDERSTANDING SAMPLE

(CT:IAH-2; 03-12-2007)

SENSITIVE BUT UNCLASSIFIED

MEMORANDUM OF UNDERSTANDING (OR AGREEMENT)

Between "Organization A"
and
"Organization B"

(ORGANIZATIONAL SEAL[S] HERE)

(DATE HERE)

(Organization A)
(Organization B)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

MEMORANDUM OF UNDERSTANDING (OR AGREEMENT)

SUPERSEDES: (None or document title and date)

INTRODUCTION

The purpose of this memorandum is to establish a management agreement between “Organization A” and “Organization B” regarding the development, management, operation, and security of a connection between "System A," owned by Organization A, and "System B,” owned by Organization B. This agreement will govern the relationship between Organization A and Organization B, including designated managerial and technical staff, in the absence of a common management authority.

AUTHORITY

The authority for this agreement is based on "Proclamation A" issued by the Secretary of the "Agency" on (date).

BACKGROUND

It is the intent of both parties to this agreement to interconnect the following information technology (IT) systems to exchange data between "ABC database" and "XYZ database." Organization A requires the use of Organization B's ABC database, and Organization B requires the use of Organization A's XYZ database, as approved and directed by the Secretary of Agency in Proclamation A. The expected benefit of the interconnection is to expedite the processing of data associated with "Project R" within prescribed timelines.

Each IT system is described below:

SYSTEM A

– Name
– Function
– Location
– Description of data, including sensitivity or classification level

SYSTEM B

– Name
– Function
– Location
– Description of data, including sensitivity or classification level

SENSITIVE BUT UNCLASSIFIED

COMMUNICATIONS

Frequent formal communications are essential to ensure 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 System A and System B agree to designate and provide contact information for technical leads for their respective system, and to facilitate direct contacts between technical leads to support the management and operation of the interconnection. To safeguard the confidentiality, integrity, and availability of the connected systems and the data they 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 e-mail when a security incident(s) is detected, so the other party may take steps to determine whether its system has been compromised and to take appropriate security precautions. The system owner will receive formal notification in writing within five (5) business days after detection of the incident(s).

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

Material Changes to System Configuration: Planned technical changes to the 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 one (1) month of implementation.

New Interconnections: The initiating party will notify the other party at least one (1) month before it connects its IT system with any other IT 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, both parties will provide notification of any changes in point of contact information. Both parties also will 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 both 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. Both parties must consent before implementing changes, and ordinarily not before the ISA has been renegotiated. Signatories to the ISA shall be the DAA for each system.

SECURITY

Both parties agree to work together to ensure the joint security of the connected systems and the data they store, process, and transmit, 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.

PRIVACY CONSIDERATIONS

Both parties agree to take measures to protect any personally identifiable information involved in the processing of information under this agreement in accordance with applicable law and Department of State procedures.

COST CONSIDERATIONS

Both 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 both 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 one (1) year after the last date on either party's signature in the signature block below. After one (1) year, 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 should explicitly supersede this agreement, which should be referenced by title and date. If one or both of the parties wish to terminate this agreement prematurely, they may do so upon 30 days' 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 (or Agreement).

(Organization A Official)	(Organization B Official)
_____	_____
(Signature and Date)	(Signature and Date)

5 FAH-11 EXHIBIT H-823 SYSTEM INTERCONNECTION IMPLEMENTATION PLAN GUIDE

(CT:IAH-2; 03-12-2007)

This exhibit provides guidance for developing a System Interconnection Implementation Plan.

1. Introduction

This section should describe the purpose and scope of the implementation plan and identify policy requirements or guidance on which the system interconnection is based. Identify the IT systems that will be interconnected, the parties that own them, and the purpose of the interconnection. Describe the service(s) that will be offered over the interconnection.

2. System Interconnection Description

Describe the architecture for the interconnection, including security controls, hardware, software, servers, and applications. Provide a diagram of the interconnection showing all relevant components.

2.1 Security Controls

Identify and describe the security controls that are currently in place for the IT systems that will be interconnected. Identify the threats that could compromise the system interconnection, and describe the existing (or planned) security controls that are configured to mitigate the threats.

2.2 System Hardware

Identify and describe the hardware that is currently used on the systems that will be interconnected, and describe how it will support the interconnection.

2.3 Software

Identify and describe the software that is currently used on the systems that will be interconnected, and describe how it will support the interconnection.

2.4 Data/Information Exchange

Identify the type(s) of data that will be exchanged between the parties, and describe the data transmission method. Identify how the data will be stored and processed. Provide a data flow diagram.

2.5 Services and Applications

Describe the services and applications that the parties will provide over the interconnection as well as any new services or applications that will be developed both initially and anticipated after the establishment of the interconnection.

3. Roles and Responsibilities

Identify the personnel who will establish and maintain the system interconnection, and define their respective roles and responsibilities. Also, identify the responsibilities of the staff authorized to use the interconnection after it is established (i.e., the users).

4. Tasks and Procedures

Provide a step-by-step approach to establishing the interconnection, based on a series of tasks and procedures. A list of recommended tasks follows:

4.1 Implement Security Controls

Provide procedures for configuring current controls and, if necessary, implement new controls. Security controls may include firewalls, identification and authentication mechanisms, logical access controls, encryption devices, intrusion detection devices, and physical security measures.

4.2 Install Hardware and Software

Provide procedures for configuring or installing hardware and software to establish the interconnection, if required.

4.3 Integrate Applications

Provide procedures for linking applications across the interconnection, if required. Also, provide procedures for developing and implementing new applications, if required.

4.4 Conduct a Risk Assessment

Describe the process of conducting an assessment to identify risks. Include a discussion as to how risks will be addressed.

4.5 Conduct Operational and Security Testing

Provide detailed test procedures to verify whether or not the interconnection operates efficiently and securely. Also, define how the results of the testing will be measured, and how deficiencies will be addressed or rectified.

4.6 Conduct Security Training and Awareness

Describe how training requirements will be addressed. A training and awareness program should be developed for all personnel who will be authorized to manage, use, and/or operate the system interconnection, including any new computer applications associated

with the interconnection.

5. Schedule and Budget

Provide a schedule for establishing the interconnection, including the estimated time required to complete each task associated with finalizing the interconnection. Also, define a budget for the project, and describe how costs will be apportioned between the participating parties, if required.

6. Documentation

Cite or include all documentation that is relevant for establishing the interconnection, including systems security plans, design specifications, and standard operating procedures.