
NIST Special Publication X-X

**Guide for Interconnecting
Information Systems**

NIST

**National Institute of
Standards and Technology**

Technology Administration
U.S. Department of Commerce

Joan Hash, Tim Grance, Steven Peck, Jonathan Smith,
Karen Korow-Diks

C O M P U T E R S E C U R I T Y

DRAFT
November 2001



Acknowledgements

The authors wish to thank the U.S. Customs Service for use of the System Interconnection Service Agreement (ISA) guidance document and sample ISA, which are contained in this document.

TABLE OF CONTENTS

1. INTRODUCTION	1
1.1 AUTHORITY	1
1.2 PURPOSE	1
1.3 SCOPE	1
1.4 AUDIENCE	1
1.5 OTHER APPROACHES TO SYSTEM INTERCONNECTIVITY	1
1.6 DOCUMENT STRUCTURE	2
2. BACKGROUND	3
3. PLANNING A SYSTEM INTERCONNECTION	5
3.1 STEP 1: ESTABLISH A JOINT PLANNING TEAM	5
3.2 STEP 2: DEFINE THE BUSINESS CASE	5
3.4 STEP 3: PERFORM CERTIFICATION AND ACCREDITATION	6
3.4 STEP 4: DETERMINE INTERCONNECTION REQUIREMENTS	6
3.5 STEP 5: DOCUMENT INTERCONNECTION AGREEMENT	9
3.6 STEP 6: APPROVE OR REJECT SYSTEM INTERCONNECTION	10
4. ESTABLISHING A SYSTEM INTERCONNECTION	12
4.1 STEP 1: DEVELOP AN IMPLEMENTATION PLAN	12
4.2 STEP 2: EXECUTE THE IMPLEMENTATION PLAN	13
4.3 STEP 3: UPDATE SYSTEM SECURITY PLANS	16
5. MAINTAINING A SYSTEM INTERCONNECTION	18
5.1 MAINTAIN CLEAR LINES OF COMMUNICATION	18
5.2 MAINTAIN EQUIPMENT	19
5.3 MANAGE USER PROFILES	19
5.4 CONDUCT SECURITY REVIEWS	19
5.5 ANALYZE AUDIT LOGS	19
5.6 REPORT AND RESPOND TO SECURITY INCIDENTS	20
5.7 COORDINATE DISASTER RESPONSE AND RECOVERY ACTIVITIES	20
5.8 PERFORM CHANGE MANAGEMENT	20
5.9 MAINTAIN SYSTEM SECURITY PLANS	21
6. DISCONNECTING A SYSTEM INERCONNECTION	22
6.1 PLANNED DISCONNECTION	22
6.2 EMERGENCY DISCONNECTION	22
6.3 RESTORATION OF INTERCONNECTION	23

APPENDIXES

APPENDIX A—INTERCONNECTION SECURITY AGREEMENT.....24
APPENDIX B—MEMORANDUM OF UNDERSTANDING/AGREEMENT32
APPENDIX C—SYSTEM INTERCONNECTION IMPLEMENTATION PLAN38
APPENDIX D—REFERENCES41

LIST OF FIGURES

FIGURE 2-1. INTERCONNECTION COMPONENTS3
FIGURE 3-1. STEPS TO PLAN A SYSTEM INTERCONNECTION.....5
FIGURE 4-1. STEPS TO ESTABLISH A SYSTEM INTERCONNECTION12
FIGURE A-1. ISA SAMPLE29
FIGURE B-1. MOU/A SAMPLE.....34

1. INTRODUCTION

1.1 AUTHORITY

The guidelines specified herein are consistent with the requirements specified in the Office of Management and Budget (OMB) Circular A-130, Appendix III, for system interconnection and information sharing. The guidelines are not mandatory. They shall not contradict existing standards, guidelines, or procedures used by Federal Government agencies for system interconnections, nor shall they contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under his statutory authority.

Nongovernmental (private sector) organizations may use the guidelines on a voluntary basis. This document is not subject to copyright.

1.2 PURPOSE

This document provides guidance for planning, establishing, maintaining, and terminating interconnections between information systems that are owned and operated by different organizations, including organizations within the same Federal agency.

1.3 SCOPE

This document is published by the National Institute of Standards and Technology (NIST) as recommended guidance for Federal agencies. It also may be used by private sector organizations. This document presents general guidelines for interconnecting information systems, including general support systems and major applications. Organizations are not expected to implement all of the guidelines herein; they should consider the guidelines in the context of their own requirements.

This document does not address classified systems or data, and it should not be used for guidance on securing such systems. Federal agencies should rely on applicable laws, regulations, and policies for interconnecting systems that are used to store, process, or transmit classified data.

1.4 AUDIENCE

This document is intended for system owners, data owners, program managers, security officers, system architects, system administrators, and network administrators who are responsible for planning, approving, establishing, maintaining, or terminating system interconnections. It is written in nontechnical language for use by a broad audience. It does not address specific information technologies.

1.5 OTHER APPROACHES TO SYSTEM INTERCONNECTIVITY

This document provides a recommended approach for interconnecting information systems. It is recognized, however, that many organizations have interconnected information systems using

different approaches, and some organizations follow specific procedures to meet unique operational requirements.

This document is intended only as guidance and it should not be construed as defining the only approach possible. It provides a logical framework for those organizations that have not previously interconnected information systems, and it provides information that other organizations may use to enhance the security of existing interconnections. Organizations should tailor the guidelines to meet their specific needs and requirements.

1.6 DOCUMENT STRUCTURE

This document is organized into five sections. Section 1 introduces the document. Section 2 describes the benefits of interconnecting information systems, identifies types of system interconnections, and explains the risks of interconnecting systems.

Sections 3 through 6 address the interconnection lifecycle. Section 3 presents a series of recommended steps for planning a system interconnection. Section 4 provides recommended steps for establishing the interconnection. Section 5 provided recommended steps for maintaining the interconnection after it is established. Section 6 provides guidelines for terminating the interconnection, as well as restoring it after it is terminated.

Appendix A provides a guide for developing an Interconnection Security Agreement, which documents the technical requirements of the interconnection, as well as a sample agreement. Appendix B provides a guide for developing a Memorandum of Understanding/Agreement, which defines the responsibilities of the participating organizations, as well as a sample memorandum. Appendix C provides a guide for developing a System Interconnection Implementation Plan. Appendix D contains a list of references.

2. BACKGROUND

A system interconnection is defined as the direct connection of two or more information systems for sharing data and other information resources. Organizations can realize significant benefits by interconnecting their information systems, such as reduced operating costs, greater functionality, improved efficiency, and centralized access to data. Interconnecting information systems may also deepen ties among participating organizations by promoting cooperation and communication.

Organizations choose to interconnect their information systems for a variety of reasons, depending on Executive or Congressional mandates or their own organizational requirements. For example, organizations may interconnect their information systems to—

- Exchange data and information among selected users
- Provide customized levels of access to proprietary databases
- Collaborate on joint projects
- Provide 24/7 communications
- Provide online training
- Provide secure storage of critical data and backup files.

A system interconnection has three basic components: two information systems (System A and System B) and the mechanism by which they are joined (the “pipe” through which data is made available, exchanged, or passed one way only). The components are shown in Figure 2-1. In this document, it is assumed that System A and System B operate under different management and are owned by different organizations, including organizations within the same agency.

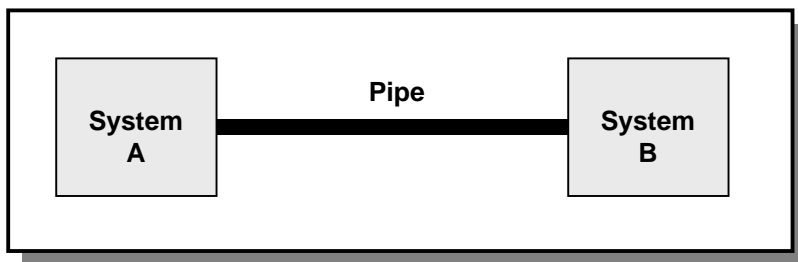


Figure 2-1. Interconnection Components

Organizations can connect their information systems using a dedicated line that is owned by one of the organizations or is leased from a third party (e.g., an Integrated Services Digital Network [ISDN], T1, or T3 line). The private or leased line is the pipe that connects the information systems. In many cases, this solution is expensive, but it can provide a high level of security for the interconnected systems because the line can be breached only through a direct physical intrusion, such as a telephone tap.

A less expensive alternative for many organizations is to connect systems over a public network (e.g., the Internet), using a virtual private network (VPN). A VPN is a data network that enables two or more parties to communicate securely across a public network by creating a private connection, or “tunnel,” between them. This replaces the need to rely on privately owned or leased lines. Data transmitted over a public network can be intercepted by unauthorized parties, however, necessitating the use of encryption to ensure data confidentiality and integrity.

There are varying levels of a system interconnection. As with any form of system access, the extent to which a party may access data and information resources is dependent on its business and security needs. Accordingly, some organizations may choose to establish a limited interconnection, whereby users are restricted to a single application or file location. Alternately, organizations may establish a broader interconnection, enabling users to access multiple applications or databases. Finally, some organizations may permit full transparency and access across their respective enterprises via the interconnection.

Despite the advantages, interconnecting information systems can expose the participating organizations to risk. If the interconnection is not properly designed, security failures could result in the compromise of the connected systems and the data they store, process, or transmit. Similarly, if one of the connected systems is compromised, the interconnection could be used as a conduit to compromise the other system and its data. The potential for compromise is underscored by the fact that, in most cases, the participating organizations have little or no control over the operation and management of the other party’s system.

It is critical, therefore, that both parties learn as much as possible about the risks associated with the planned or current interconnection and the security controls they can implement to mitigate those risks. In addition, it is critical that they establish an agreement between themselves regarding the management, operation, and use of the interconnection and that they formally document this agreement.

Federal policy requires Federal agencies to establish interconnection agreements. Specially, OMB Circular A-130, Appendix III, requires agencies to obtain written management authorization before connecting their information systems to other systems, based on an acceptable level of risk. The written authorization should define the rules of behavior and controls that must be maintained for the system interconnection, and it should be included in the organization’s system security plan. Similarly, the Government Information Security Reform Act (GISRA) requires Federal agencies to develop and implement security programs that protect their information operations and assets, including operations and assets that are provided or managed by other agencies (i.e., through an interconnection).

3. PLANNING A SYSTEM INTERCONNECTION

The process of connecting two or more information systems should begin with a planning phase, in which the participating organizations perform preliminary activities and examine all relevant technical, security, and administrative issues. The planning phase ensures that the interconnection will operate as efficiently and securely as possible. This section discusses recommended steps for planning a system interconnection, as depicted in Figure 3-1.

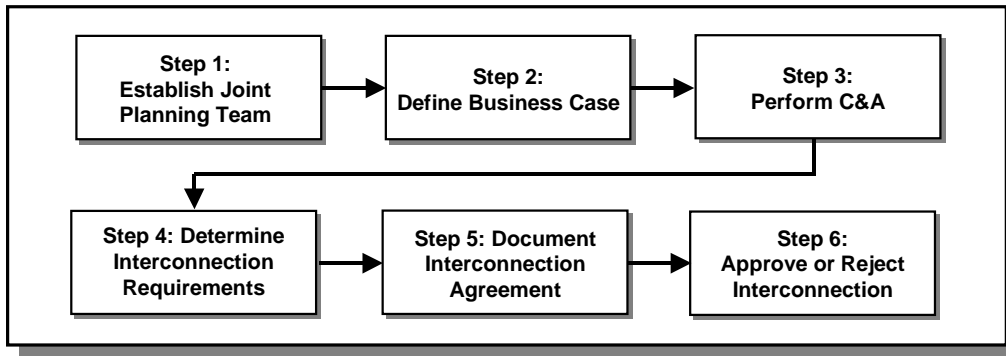


Figure 3-1. Steps to Plan a System Interconnection

3.1 STEP 1: ESTABLISH A JOINT PLANNING TEAM

Both organizations are responsible for ensuring the security of their respective systems and data. Essential to this goal is a well-coordinated approach to interconnectivity, including regular communications between the organizations throughout the life cycle of the interconnection. Therefore, the organizations should consider establishing a joint planning team composed of appropriate managerial and technical staff, including program managers, security officers, system administrators, network administrators, and system architects.

The joint planning team could be part of an existing forum or it could be created specifically for the planned interconnection. Regardless of how it is formed, the team must have the commitment and support of the system and data owners and other appropriate senior managers. The team would be responsible for coordinating all aspects of the planning process and ensuring that it had clear direction and sufficient resources. In addition, the team could remain active beyond the planning phase, to serve as a forum for future discussions about issues involving the interconnection.

3.2 STEP 2: DEFINE THE BUSINESS CASE

Both organizations 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. Defining the business case will establish the basis of the interconnection and facilitate the planning process. Factors that should be considered include likely costs (e.g., staffing, equipment, and facilities), expected benefits (e.g., improved efficiency, centralized access to data), and potential risks (e.g., technical, legal, and financial).

As part of this process, both organizations should examine privacy issues related to data that will be exchanged or passed over the interconnection, and determine whether such use is restricted under current statutes, regulations, or policies. Examples of data that might be restricted include personally identifiable information such as names and social security numbers, or confidential business information such as contractor bid rates and trade secrets. Each organization should consult with its Privacy Officer or Legal Counsel to determine whether such information may be shared or transferred. Permission to exchange or transfer data should be documented, along with a commitment to protect such data.

3.4 STEP 3: PERFORM CERTIFICATION AND ACCREDITATION

Before interconnecting their information systems, each organization should ensure that its respective system is properly certified and accredited in accordance with Federal certification and accreditation (C&A) standards. Certification involves testing and evaluating the technical and nontechnical security features of the system to determine the extent to which it meets a set of specified security requirements. Accreditation is the official approval by a Designated Approving Authority (DAA) or other authorizing management official that the system may operate for a specific purpose using a defined set of safeguards at an acceptable level of risk.

The C&A process is applicable for both emerging systems and those already in production. See NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, and NIST Special Publication 800-37, *Certification and Accreditation Guidelines (Draft)*, for guidance on performing a C&A.

3.4 STEP 4: DETERMINE INTERCONNECTION REQUIREMENTS

The joint planning team should identify and examine all relevant technical, security, and administrative issues surrounding the interconnection. This information will be used to develop an Interconnection Security Agreement (ISA) and a Memorandum of Understanding or Agreement (MOU/A). This information also will be used to develop an implementation plan for establishing the interconnection.

The joint planning team should consider the following issues:

- *Level and Method of Interconnection:* Define the level of interconnectivity that will be established between the information systems, ranging from limited connectivity (limited data exchange) to enterprise-level connectivity (active sharing of data and applications). In addition, describe the method used to connect the systems (dedicated line or VPN).
- *Impact on Existing Infrastructure and Operations:* Determine whether the network or computer infrastructure currently used by both organizations is sufficient to support the interconnection, or whether additional components are required (e.g., communication lines, routers, switches, servers, and software). If additional components are required, determine the potential impact that installing and using them might have on the existing infrastructure, if any. In addition, determine the potential impact the interconnection

could have on current operations, including new demands on system administration, increases in data traffic, and new training requirements.

- *Hardware Requirements:* Identify hardware that will be needed to support the interconnection, including communications lines, routers, firewalls, hubs, switches, servers, and computer workstations. Determine whether existing hardware is sufficient, or whether additional components are required. If new hardware is required, select appropriate products that ensure interoperability.
- *Software Requirements:* Identify software that will be needed to support the interconnection, including software for firewalls, servers, and computer workstations. Determine whether existing software is sufficient, or whether additional software is required. If new software is required, select appropriate products that ensure interoperability.
- *Data Sensitivity:* Identify the sensitivity level of data or information resources that will be made available, exchanged, or passed one way only across the interconnection. Identifying data sensitivity is critical for determining the security controls that should be used to protect the connected systems and data. Examples of sensitive data include financial data, personal information, and proprietary business data. See NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, for further guidance.
- *User Community:* Define the community of users who will access, exchange, or receive data across the interconnection. Determine whether users must possess certain characteristics corresponding to data sensitivity levels, such as employment status or nationality requirements. Devise an approach for compiling and managing the profiles of all users who will have access to the interconnection, including user identifications, workstation addresses, workstation type, operating system, and any other relevant information. Each organization should use this information to develop and maintain a comprehensive database of its users.
- *Services and Applications:* Identify the information services that will be provided over the interconnection by each organization and the applications associated with those services, if appropriate. Examples of services include e-mail, file transfer protocol (FTP), RADIUS, Kerberos, database query, file query, and general computational services.
- *Security Controls:* Identify security controls that will be implemented to protect the confidentiality, integrity, and availability of the systems and data that pass between them. Controls can be selected from the examples provided in Section 4 or from other sources. Controls should be appropriate for the systems that will be connected and the environment in which the interconnection will operate.
- *Segregation of Duties:* Determine whether the management or execution of certain duties should be divided between two or more individuals. Examples of duties that might be segregated include auditing, managing user profiles, and maintaining equipment.

Segregation of duties reduces the risk that a single individual could cause harm to the connected systems and data, either accidentally or deliberately.

- *Incident Reporting and Response:* Establish procedures to report and respond to anomalous and suspicious activity that is detected by either technology or staff. Determine when and how to notify each other about security incidents that could affect the interconnection. Identify the types of information that will be reported, including the cause of the incident, affected data or programs, and actual or potential impact. In addition, identify types of incidents that require a coordinated response, and determine how to coordinate response activities. It might be appropriate to develop a joint incident response plan for this purpose. See NIST Special Publication 800-3, *Establishing a Computer Security Incidence Response Capability*, for further information.
- *Data Backup:* Determine whether data or information that is passed across the interconnection must be backed up and stored. If backups are required, identify the types of data that will be backed up, how frequently backups will be conducted (daily, weekly, or monthly), and whether backups will be performed by both parties or only one party. Also, determine how to perform backups, and link backup procedures to disaster response and recovery procedures. Critical data should be backed up regularly and stored in an off-site location to prevent loss or damage. In addition, audit logs should be copied and stored in a secure location to prevent theft, damage, or tampering.
- *Contingency Planning:* Each organization should have a contingency plan(s) to respond to and recover from disasters and other disruptive contingencies, ranging from the failure of system components to the loss of computing facilities. Determine how to notify each other of such contingencies, the extent to which the organizations will assist each other, and the terms under which assistance will be provided. Determine whether to incorporate redundancy into components supporting the interconnection, including redundant interconnection points, and how to retrieve data backups. Coordinate disaster response training, testing, and exercises. See NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems (Draft)*, for more information.
- *Data Element Naming and Ownership:* Determine whether the data element naming schemes used by both organizations are compatible, or whether new databases must be normalized so the organizations can use data passed over the interconnection. In addition, determine whether ownership of data is transferred from the transmitting party to the receiving party, or whether the transmitting party retains ownership and the receiver becomes the custodian. As part of this effort, determine how transferred data will be stored, whether they may be re-used, and how they will be destroyed.
- *Change Management:* Determine how to coordinate the planning, design, and implementation of changes that could affect the connected systems or data, such as upgrading hardware or software, or adding services. Consider establishing a forum with appropriate staff from each organization to review proposed changes to the interconnection. Coordinating change management activities will reduce the potential for

implementing changes that could disrupt the availability or integrity of data, or introduce vulnerabilities.

- *Rules of Behavior:* Develop rules of behavior that clearly delineate the responsibilities and expected behavior of all personnel who will have access to the interconnection. The rules should be in writing and they should state the consequences of inconsistent behavior or noncompliance. The rules will form the basis for security awareness and training.
- *Security Awareness and Training:* Define a security awareness and training program for all personnel who will be involved in the management, use, and operation of the interconnection. The program may be incorporated into current security awareness and training. Identify training requirements, including frequency and scheduling, and assign responsibility for conducting training and awareness activities. Design training to ensure personnel are familiar with the rules of behavior associated with the interconnection. Require users to sign an acknowledgement form indicating that they understand the rules, if appropriate. If shared applications are used, ensure users know how to use them properly. If the interconnection is used to exchange or transfer sensitive data, ensure that users understand special requirements for handling such data, if required. See NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, for guidance.
- *Roles and Responsibilities:* Identify personnel who will be responsible for establishing, maintaining, or managing the interconnection, including managers, system administrators, application designers, auditors, security staff, and specialists from such fields as insurance and risk management. Choose personnel who have appropriate subject matter expertise. If contractors are involved, one or both organizations may be required to develop a nondisclosure agreement to safeguard the confidentiality and integrity of exchanged data.
- *Scheduling:* Develop a preliminary schedule for all activities involved in planning, establishing, and maintaining the interconnection. Also, determine the schedule and conditions for terminating or reauthorizing the interconnection. For example, both parties might agree to review the interconnection every 12 months to determine whether to reauthorize it for continued operation.
- *Costs and Budgeting:* Identify the expected costs required to plan, establish, and maintain the interconnection. Identify all associated costs, including labor, hardware, software, communications lines, applications, facilities, physical security, training, and testing. Develop a comprehensive budget, and determine how costs will be apportioned between the parties, if required.

3.5 STEP 5: DOCUMENT INTERCONNECTION AGREEMENT

The joint planning team should document not only an agreement governing the interconnection, but also the terms under which the organizations will abide by the agreement, based on its review of all relevant technical, security, and administrative issues (Step 4 above). Two documents may

be developed: an Interconnection Security Agreement (ISA) and a Memorandum of Understanding (or Agreement) (MOU/A), discussed below.

Because the ISA and the MOU/A may contain sensitive information, they should be stored in a secure location to protect against theft, damage, or destruction. If copies are stored electronically, they should be protected from unauthorized disclosure or modification. An ISA development guide and sample are provided in Appendix A, and an MOU/A development guide and sample are provided in Appendix B.

3.5.1 Substep 1: Develop an Interconnection Security Agreement

The ISA is a security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. It also supports the MOU/A between the organizations. Specifically, the ISA documents the requirements for connecting the information systems, describes the security controls that will be used to protect the systems and data, contains a topological drawing of the interconnection, and provides a signature block.

3.5.2 Substep 2: Establish a Memorandum of Understanding (or Agreement)

The MOU/A documents the terms and conditions for sharing data and information resources in a secure manner. Specifically, the MOU/A defines the purpose of the interconnection; identifies relevant authorities; specifies the responsibilities of both organizations; and defines the terms of agreement, including apportionment of costs and the timeline for terminating or reauthorizing the interconnection. The MOU/A should not include technical details on how the interconnection is established or maintained; that is the function of the ISA.

3.6 STEP 6: APPROVE OR REJECT SYSTEM INTERCONNECTION

The joint planning team should submit the ISA and the MOU/A to the DAA or other authorizing management official of each organization, requesting approval for the interconnection. (In some cases, the DAA will be the system owner.) Upon receipt, the DAAs should review the ISA, the MOU/A, and any other relevant documentation. Based on this review, the DAAs should decide on one of the following:

- Approve the interconnection
- Grant interim approval
- Reject the interconnection.

If the DAAs (or other authorizing officials) accept the ISA and the MOU/A, they should sign and date the documents, thereby approving the interconnection. The documents should then be given to an appropriate security officer from each organization to retain. A signed copy of the documents may also be forwarded to the appropriate system program manager within each organization.

One or both DAAs may decide to grant an interim approval. Interim approval may be granted if the planned interconnection does not meet the requirements stated in the ISA, but mission criticality requires that the interconnection must be established. The DAA(s) should provide a signed letter to the respective security officers specifying the tasks that must be completed before full approval will be granted, including the implementation of additional security controls, if required. In addition, the DAA(s) should specify timelines for completing the tasks, although the tasks should be completed before the interconnection is operational. The joint planning team should then work to meet the requirements specified by the DAA(s).

If one or both DAAs reject the interconnection, the joint planning team should return to the planning process. In this situation, the DAA(s) should provide a signed letter to the respective security officers specifying the reason(s) for rejecting the planned interconnection and provide suggested solutions. The DAA(s) also should meet with the joint planning team to discuss and agree on the proposed solutions and timelines for correcting specified deficiencies, so approval may be granted.

4. ESTABLISHING A SYSTEM INTERCONNECTION

After the system interconnection is planned and approved, it must be implemented. This section provides recommended steps for establishing the system interconnection, as shown in Figure 4-1.

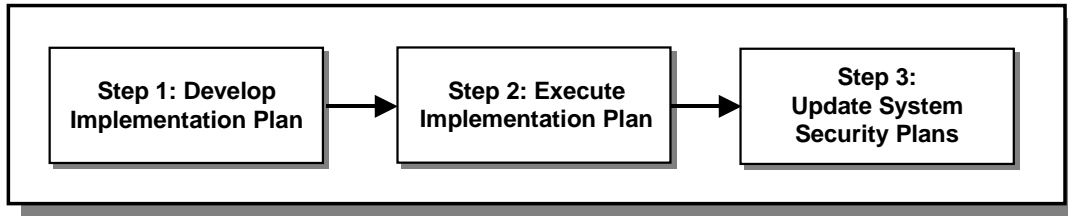


Figure 4-1. Steps to Establish a System Interconnection

4.1 STEP 1: DEVELOP AN IMPLEMENTATION PLAN

To ensure that the information systems are connected properly and securely, the joint planning team should 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 technical requirements specified in the ISA will be implemented. A well-developed implementation plan will greatly improve the likelihood that the interconnection will operate successfully and securely.

At a minimum, the implementation plan should—

- Describe the information systems that will be connected
- Identify the sensitivity or classification level of data that will be made available, exchanged, or passed one way across the interconnection
- Identify personnel who will establish and maintain the interconnection, and clearly specify their responsibilities
- Identify implementation tasks and procedures
- Identify and describe security controls that will be used to protect the confidentiality, integrity, and availability of the connected systems and data
- Provide test procedures and measurement criteria to ensure the interconnection operates properly and securely
- Specify training requirements for users, including a training schedule.

A guide for developing an implementation plan is provided in Appendix C.

4.2 STEP 2: EXECUTE THE IMPLEMENTATION PLAN

After the implementation plan is developed, it must be executed. A list of recommended tasks for establishing an interconnection is provided below. Detailed procedures associated with each task should be provided in the implementation plan.

4.2.1 Substep 1: Implement or Configure Security Controls

If security controls are not in place or they are configured improperly, the process of establishing the interconnection could expose the information systems to access by unauthorized personnel. Therefore, the first step is to implement appropriate security controls or configure existing controls, as specified in the ISA. Security controls may include the following:

- *Firewalls:* Firewalls determine whether data packets are permitted into a network, and they restrict access to specific resources. Install firewalls to protect internal networks and other resources from unauthorized access across the interconnection, or configure existing firewalls accordingly. If the interconnection involves the use of servers, host them in a separately protected “demilitarized zone” (DMZ), which may be accomplished by installing two firewalls: one on the external line and one at the connection to internal networks. (Alternately, a firewall could be installed on the external line and a security portal installed at the internal connection.) Ensure that firewall ports are configured correctly with access controls, policies, and procedures, and change all default passwords.
- *Intrusion Detection:* An intrusion detection system (IDS) detects security breaches by looking for anomalies in normal activities, by looking for patterns of activity that are associated with intrusions or insider misuse, or both. One or both organizations should implement an IDS (or configure existing IDSs) to detect undesirable or malicious activity that could affect the interconnection or data that pass over it. A combination of network-based and host-based IDSs may be used, if appropriate. Configure alert mechanisms to notify system administrators or security officers when intrusions or unusual activities are detected. See NIST Special Publication 800-31, *Intrusion Detection Systems*, for further information.
- *Auditing:* Install or configure mechanisms to record activities occurring across the interconnection, including application processes and user activities. Activities that should be recorded include event type, date and time of event, user identification, workstation identification, the success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs should have read-only access, and only authorized personnel should have access to the logs. In addition, logs should be stored in a secure location to protect against theft and damage.
- *Identification and Authentication:* Identification and authentication is used to prevent unauthorized personnel from entering an information system. Implement strong mechanisms to identify and authenticate users to ensure that they are authorized to access the interconnection. Mechanisms include user identification and passwords, digital

certificates, authentication tokens, biometrics, and smart cards. If used, passwords should be at least six to eight characters long, should have a mixture of alphabetic and numeric characters, and should be changed regularly. Master password files should be encrypted and securely protected from unauthorized access. If digital signatures are used, the technology must conform to Federal Information Processing Standard (FIPS) 186-2, *Digital Signature Standard (DSS)*.¹

Depending on data sensitivity, organizations may permit users to access the interconnection after they have authenticated to their local domain, reducing the need for multiple passwords or other mechanisms. Applications operating across the interconnection could rely on authentication information from the user's local domain, using a proxy authentication mechanism.

- *Logical Access Controls:* Logical access controls are mechanisms used to designate who has access to system resources and the types of transactions and functions they are permitted to perform. Use access control lists (ACL) and access rules to specify the access privileges of authorized personnel, including the level of access and the types of transactions and functions that are permitted (e.g., read, write, execute, delete, create, and search). Hardware and software often are configured with ACLs, or the ACLs may be administered offline and then distributed to routers and other devices. Configure access rules to grant appropriate access privileges to authorized personnel, based on their roles or job functions. Ensure only system administrators have access to the controls. In addition, install a log-on warning banner notifying unauthorized users that they have accessed a Federal Government computer system and unauthorized use can be punishable by fines or imprisonment. Acceptance of the banner should constitute consent to monitoring.
- *Virus Scanning:* Data and information that pass from one information system to the other should be scanned with antivirus software to detect and eliminate malicious code, including viruses, worms, and Trojan horses. Install antivirus software on all servers and computer workstations linked to the interconnection. Ensure the software is automatically updated and properly maintained with current virus definitions. In addition, incorporate antivirus scanning into user training, to ensure that users understand how to scan computers, file downloads, and e-mail attachments, if appropriate. Develop procedures and assign responsibilities for responding to and recovering from malicious code attacks.
- *Encryption:* Encryption is used to ensure that data cannot be read or modified by unauthorized users. When used properly, encryption will protect the confidentiality and integrity of data during transmission and storage, and it may be used for authentication and nonrepudiation. Encryption may be implemented in devices such as routers, switches, firewalls, servers, and computer workstations. Configure devices to apply the appropriate level of encryption required for data that pass over the interconnection. If required, implement encryption mechanisms (e.g., digital signatures) to authenticate users

¹ This requirement applies only to Federal agencies.

to the interconnection and to shared applications, and to provide nonrepudiation.

- *Physical and Environmental Security:* Physical security addresses the physical protection of computer hardware and software. Place hardware and software supporting the interconnection, including interconnection points, in a secure location that is protected from unauthorized access, interference, or damage. Ensure that environmental controls are in place to protect against hazards such as fire, water, and excessive heat and humidity. In addition, place computer workstations in secure areas to protect them from damage, loss, theft, or unauthorized physical access. Consider using access badges, cipher locks, or biometric devices to control access to secure areas. For guidance, see NIST Special Publications 800-12, 800-30, and 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*.

4.2.2 Substep 2: Install or Configure Hardware and Software

After security controls are installed or configured, it may be necessary to install hardware and software to establish the interconnection, or to configure existing hardware and software for this purpose, if appropriate. Place hardware and software in secure areas that are configured with proper environmental controls. Equipment that might be required includes the following:

- *Communications Line:* If a dedicated line is used for the interconnection, ensure the line is connected to the appropriate physical site at each organization.
- *VPN:* Install VPN software on servers and local workstations, and configure it appropriately.
- *Routers and Switches:* Install routers or switches to connect to the communications line between the information systems, or configure existing devices.
- *Hubs:* Install hubs to join multiple computers into a single network segment, if required.
- *Servers:* Install appropriate servers to support services provided across the interconnection, such as database, Web, and application servers. If existing servers are used, determine whether the hardware should be upgraded to support the interconnection, and whether the latest software and security patches have been applied.
- *Computer Workstations:* Configure computer workstations by providing a menu option or a link to enable authorized users to invoke the interconnection. Install appropriate client software, if required.

4.2.3 Substep 3: Integrate Applications

Integrate applications or protocols for services that are provided across the interconnection. Examples include word processing, database applications, e-mail, Web browsers, application servers, authentication servers, domain servers, development tools, editing programs, and communications programs.

4.2.4 Substep 4: Conduct Operational and Security Testing

Conduct a series of tests to ensure equipment operates properly and there are no obvious ways for unauthorized users to circumvent or defeat security controls. Test the interface between applications across the interconnection, and simulate data traffic at planned activity levels to verify correct translation at the receiving end(s). Test security controls under realistic conditions. Document the results of the testing and compare them to a set of predetermined operational and security standards approved by both organizations. Correct errors or problems and document the actions taken. Retest the interconnection to ensure errors or problems are eliminated and new flaws have not been introduced.

4.2.5 Substep 5: Conduct a Risk Assessment

Conduct a risk assessment to identify vulnerabilities and threats associated with the interconnection and to determine the corresponding level of risk. The assessment may be performed by a certified third party, if appropriate. Base the assessment on a set of predetermined security requirements approved by the both organizations, and document the results. Adjust security controls to mitigate identified risks, and implement additional controls, if required. Document the corrective actions taken.

4.2.6 Substep 6: Conduct Security Awareness and Training

Conduct security awareness and training for all personnel who are involved in the management, use, and operation of the interconnection. Distribute the rules of behavior to all users who will have access to the interconnection, and require them to sign an acknowledgement form confirming they understand the rules before granting them authorization to access it. In addition, ensure staff know how to report suspicious or prohibited activity, and how to request assistance if they encounter problems.

4.2.7 Substep 7: Activate the Interconnection

Activate the interconnection for use by both parties, following prescribed guidelines. It is recommended that one or both organizations closely monitor the interconnection for a period of at least three months to ensure that it operates properly and securely. Analyze audit logs carefully and frequently, and monitor the types of assistance requested by users. Document any errors or problems that occur and correct them.

4.3 STEP 3: UPDATE SYSTEM SECURITY PLANS

Both organizations should update their system security plans and related documents to reflect the changed security environment in which their respective system operates. It is recommended the security plans include the following information regarding the system interconnection (and other interconnections, if appropriate):

- Names of interconnected systems

- Organization owning the other systems
- Type of interconnection
- Short discussion of major concerns or considerations in determining interconnection
- Name and title of authorizing management official(s)
- Date of authorization
- System of record, if applicable (Privacy Act data)
- Sensitivity level of each system
- Interaction among systems
- Hardware inventory
- Software inventory
- Security concerns and rules of behavior governing the interconnection.

Refer to NIST Special Publication 800-18 for further information.

5. MAINTAINING A SYSTEM INTERCONNECTION

After the interconnection is established, it must be actively maintained to ensure it operates properly and securely. This section describes recommended activities for maintaining the system interconnection, including:

- Maintain clear lines of communication
- Maintain equipment
- Manage user profiles
- Conduct security reviews
- Analyze audit logs
- Report and respond to security incidents
- Coordinate disaster response and recovery activities
- Perform change management
- Maintain system security plans.

5.1 MAINTAIN CLEAR LINES OF COMMUNICATION

It is critical that both organizations maintain clear lines of communication and communicate regularly. Open lines of communication help ensure that the interconnection is properly maintained and security controls remain effective. Open communications also facilitate change management activities by making it easy for both sides to notify each other about planned system changes that could affect the interconnection. Finally, maintaining clear lines of communication enables both sides to promptly notify each other of security incidents and system disruptions and helps them conduct coordinated responses, if necessary.

Communications should be conducted between designated personnel using approved procedures, as specified in the ISA. Information that should be shared includes the following:

- Initial agreements and changes to agreements
- Changes in designated management and technical personnel
- Activities related to establishing and maintaining the interconnection
- Change management activities that could affect the interconnection
- Security incidents that could affect the connected systems and data
- Disasters and other contingencies that disrupt one or both of the connected systems

- Planned restoration of the interconnection.

Information may be exchanged verbally or in writing, depending on the nature of the communications. However, any activities that could change, modify, or adjust one or both of the connected systems should always be communicated in writing.

5.2 MAINTAIN EQUIPMENT

One or both organizations should maintain the equipment used to operate the interconnection, to ensure its continued integrity and availability. Equipment should be maintained at regular service intervals and in accordance with manufacturer specifications. Only authorized personnel should be allowed to service and repair equipment. If vendors are used, they should be escorted and not left unattended, if required. All maintenance activities and corrective actions should be documented, and the records should be stored in a secure location. Finally, organizations should notify each other before performing maintenance activities, including scheduled outages.

5.3 MANAGE USER PROFILES

Both organizations should actively manage user profiles. If a user resigns or changes job responsibilities, the appropriate organization should update the user's profile to prevent access to data or information that is no longer appropriate. Organizations should not only consider monitoring user inactivity, but also establish procedures for investigating, disabling, and terminating access to users who do not access the interconnection over a specific period of time. For example, access privileges for users who do not access the interconnection after 30 days should be disabled, and privileges for users who do not access the interconnection within 90 days should be terminated. Such measures help prevent intruders from masquerading as legitimate users by exploiting inactive accounts.

5.4 CONDUCT SECURITY REVIEWS

One or both organizations should regularly review the security controls for the interconnection to ensure they are operating properly and are providing appropriate levels of protection. A variety of security assessment tools are available commercially that can be run against firewalls and other controls to identify administrative and configuration errors and other security problems. Penetration tests also should be conducted.

Security reviews may be conducted by designated audit authorities of one or both organizations, or by an independent third party. Both organizations should agree on the rigor and frequency of reviews as well as a reporting process. For example, both organizations should examine the results of security reviews to identify areas requiring attention. Errors or problems should be corrected in a timely manner. Corrective actions should be documented, and the records should be stored in a secure location.

5.5 ANALYZE AUDIT LOGS

One or both organizations should regularly analyze audit logs to detect and track unusual or suspicious activities across the interconnection that might indicate intrusions or internal misuse. Given the voluminous nature of audit logs, the logs should be kept at a manageable size by setting logging levels appropriately. Automated tools should be used for scanning for anomalies, unusual patterns, and known attack signatures, and tools should be configured to alert a system administrator if a threat is detected. In addition, an experienced system administrator (or more, if segregation of duties is applied) should periodically review the logs to detect patterns of suspicious activity that scanning tools might not recognize.

5.6 REPORT AND RESPOND TO SECURITY INCIDENTS

Both organizations should notify each other of intrusions, attacks, or internal misuse, so the other party can take steps to determine whether its system has been compromised. They should take appropriate steps to isolate and respond to such incidents, in accordance with their respective incident response procedures. Actions that may be taken include shutting down a computer, disabling an account, reconfiguring a router or firewall, or shutting down the system. If the incident involved personnel from one or both organizations, disciplinary actions may be required. In some cases, both parties should coordinate their actions, especially if a major security breach occurs. If the incident was an attack or an intrusion attempt, law enforcement authorities should be notified, and all attempts should be made to preserve evidence. All security incidents, along with the reporting and response actions taken, should be documented.

5.7 COORDINATE DISASTER RESPONSE AND RECOVERY ACTIVITIES

Both organizations should coordinate disaster response and recovery training, testing, and exercises to minimize the impact of disasters and other contingencies that could damage the connected systems or jeopardize the confidentiality and integrity of data. Special attention should be given to emergency alert and notification; damage assessment; and response and recovery, including data retrieval. The organizations should consider developing joint procedures based on existing contingency plans, if appropriate. Finally, the organizations should notify each other about changes to emergency point of contact information (primary and alternate), including changes in staffing, addresses, telephone and fax numbers, and e-mail addresses.

5.8 PERFORM CHANGE MANAGEMENT

Effective change management is critical to ensure the interconnection is properly maintained and secured. Each organization should establish a change control board (CCB), or a similar body, to review and approve planned changes to their respective systems, such as upgrading software or adding services. The decision to upgrade or modify a system should be based on the security requirements specified in the ISA and on determination that the change will not adversely affect the interconnection. The other party should be notified in writing and involved in this process. After approving a change, the CCB would be responsible for managing and tracking the change to ensure it did not harm the interconnection, either by disrupting service or introducing vulnerabilities.

If a planned change is designed specifically for the interconnection, both parties should establish a joint CCB or a similar body to review and approve the change. In most cases, such changes are designed to improve the operation and security of the interconnection, such as by adding new functions, improving user interfaces, and eliminating (or mitigating) known vulnerabilities. Nevertheless, it is critical that both organizations carefully review such changes before implementing them and that they manage and track the changes after they are made. Any errors or problems should be corrected in a timely manner.

5.9 MAINTAIN SYSTEM SECURITY PLANS

Both organizations should maintain their system security plans and other relevant documentation to reflect any changes to their information systems or to the interconnection. Refer to NIST Special Publication 800-18 for further information.

6. DISCONNECTING A SYSTEM INTERCONNECTION

This section describes the process for terminating the system interconnection. If possible, the interconnection should be terminated in a methodical manner to avoid disrupting the other party's information system.

6.1 PLANNED DISCONNECTION

The decision to terminate the system interconnection should be made by the system owner with the advice of appropriate managerial and technical staff. Before terminating the interconnection, the initiating party should notify the other party in writing, and it should receive an acknowledgment in return. The notification should describe the reason(s) for the disconnection, provide the proposed timeline for the disconnection, and identify technical and management staff who will conduct the disconnection.

An organization might have a variety of reasons to terminate an interconnection, including the following:

- Changed business needs
- Failed security audits, including increases in risks that rise to unacceptable levels
- Inability to abide by the technical specifications of the ISA
- Inability to abide by the terms and conditions of the MOU/A
- Cost considerations, including increases in the cost of maintaining the interconnection
- Changes in system configuration or in the physical location of equipment.

The schedule for terminating the interconnection should permit a reasonable period for internal business planning so both sides can make appropriate preparations, including notifying affected users and identifying alternative resources for continuing operations. In addition, managerial and technical staff from both organizations should coordinate to determine the logistics of the disconnection and the disposition of shared data. Finally, the disconnection should be conducted when the impact on users is minimal, such as a weekend.

6.2 EMERGENCY DISCONNECTION

If one or both organizations detect an attack, intrusion attempt, or other contingency that exploits or jeopardizes the connected systems or their data, it may be necessary to abruptly terminate the interconnection without providing written notice to the other party. This extraordinary measure should be taken only in extreme circumstances and only after consultation with appropriate technical staff and senior management.²

² If possible, the organizations should consult with their Legal Counsel before making an emergency disconnection to address issues related to liability, investigation, or evidence preservation.

The other party should be notified immediately by telephone or some other method. The decision to make an emergency disconnection should be made by the system owner and implemented by technical staff. If the system owner is unavailable, a predesignated staff member may authorize the disconnection in accordance with written criteria that stipulate the conditions under which this authority is exercised.

The system owner or designee should verbally notify the other party's emergency contact as soon as possible, either before the interconnection is terminated or immediately thereafter. Both parties should work together to isolate and investigate the incident, including conducting a damage assessment and reviewing audit logs and security controls, in accordance with incident response procedures. If the incident was an attack or an intrusion attempt, law enforcement authorities should be notified, and all attempts should be made to preserve evidence.

The initiating party should provide a written notification to the other party in a timely manner (e.g., within five days). The notification should describe the nature of the incident, explain why the interconnection was terminated, describe how the interconnection was terminated, and identify actions taken to isolate and investigate the incident.

6.3 RESTORATION OF INTERCONNECTION

Both organizations may choose to restore the system interconnection after it has been terminated. The decision to restore the interconnection should be based on the cause and duration of the disconnection. For example, if the interconnection was terminated because of an attack, intrusion, or other contingency, both parties should implement appropriate countermeasures to prevent a recurrence of the problem. They also should modify the ISA and MOU/A to address issues requiring attention, if necessary. Alternately, if the interconnection has been terminated for more than 90 days, both parties should perform a risk assessment on their respective systems, and reexamine all relevant planning and implementation issues, including developing a new ISA and MOU/A.

APPENDIX A INTERCONNECTION SECURITY AGREEMENT

The organizations that own and operate the connected information systems should develop an Interconnection Security Agreement (ISA) to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations (see Appendix B). An ISA development guide is provided below; a sample ISA is depicted in Figure A-1 at the end of this appendix.

A.1 PURPOSE

The intent of the ISA is to document and formalize the interconnection arrangements between “Organization A” and “Organization B” and to specify any details that may be required to provide overall security safeguards for the systems being interconnected. General guidance regarding the contents of an ISA is provided below; however, each ISA may be tailored by mutual consent of its originators.

Information systems owned by other Federal Government agencies and commercial process owners should be used to process data transactions only after the completion of a duly signed ISA. Systems approved by an ISA for interconnection with (name of Organization A) systems should meet the protection requirements equal to, or greater than, those implemented by the respective interconnected (name of Organization B)-owned system(s) and meet the intent of the policy prescribed herein.

A.2 REFERENCES

The authority for the interconnectivity between information systems is based on OMB Circular A-130 and a signed MOU/A between the two organizations being interconnected.

A.3 SCOPE

This procedure is effective in the following System Development Life Cycle (SDLC) phases:

CONCEPTS DEVELOPMENT	√	DEPLOYMENT	√
DESIGN	√	OPERATIONS	√
DEVELOPMENT	√	DISPOSAL	√

A.4 PROCEDURE

An ISA is used to support an MOU/A that established the requirements for data exchange between two organizations. The MOU is used to document the business requirement and all the legal jargon necessary to support the business relations between the two organizations. The MOU/A should not include technical details regarding how the interconnection is consummated;

that is the function of the ISA. An ISA is a distinct security-related document that outlines the technical solution and security requirements for the interconnection. It does not replace an MOU/A. As older MOU/As are updated, they should be changed to refer to the appropriate ISA covering the connectivity addressed by the MOU/A. Use of the ISA is compliant with other elements of the Federal Government.

An ISA can be signed only by the two Designated Approval Authorities (DAA) (or other authorizing management officials) whose names appear in Section 4 of the agreement. It should be formally signed *before the interconnection is declared operational*.

A.5 CONTENTS OF AN INTERCONNECTION SECURITY AGREEMENT

An ISA should contain a cover sheet followed by a document of four numbered sections. The information presented within those four sections should address the need for the interconnection and the security controls required and implemented to protect the confidentiality, integrity, and availability of the systems and data. The extent of the information should be sufficient that the two DAAs can make a prudent decision about approving the interconnection of the systems. The four sections are as follows:

- Section 1: Interconnection Statement of Requirements
- Section 2: Systems Security Considerations
- Section 3: Topological Drawing
- Section 4: Signatory Authority.

***NOTE:** A person from one of the organizations should take the lead for completing the ISA; however, that person should not try to determine which questions in Section 2 apply to the other system.*

It is difficult to define the required security considerations that may need to be documented without having detailed knowledge of each system being connected. The items in Section 2 should be included by mutual consent. Therefore, a technical representative from each organization who understands the system should choose which security issues are relevant in Section 2. One system may have several security requirements that need to be documented and that may not apply to the other system. The technical representative for each organization should have the authority to represent his or her DAA for defining requirements for the particular ISA.

A.6 SECTION 1: INTERCONNECTION STATEMENT OF REQUIREMENTS

Use this section to document the formal requirement for connecting the two systems. Explain the rationale for the interconnection to the two DAAs. Enter a one- or two-paragraph statement justifying the interconnection. Within the information presented, include the following information:

- The requirement for the interconnection, including the benefits derived.

- The names of the systems being interconnected.
- The agency name or organization that initiated the requirement. If the requirement is generated by some higher level agency or organization, indicate the name of the organization and the individual, if appropriate, that requested the interconnection.

A.7 SECTION 2: SYSTEM SECURITY CONSIDERATIONS

Use this section to document the security features that are in place to protect the confidentiality, integrity, and availability of the data and the systems being interconnected. The technical representative from each organization should discuss the contents on this section to come to a mutual agreement as to which items are to be included. Both organizations should answer each item, even if only one party is being affected by the subjected item. Note that some items are recommended, whereas others are optional. Optional items affecting only one system should be answered and included.

***SUGGESTED ITEMS:** (Do not include this title “Suggested Items” in the ISA.) The following items should be included and answered in the ISA:*

- *General Information/Data Description.* Describe the information and data being made available, exchanged, or passed one way only, by the interconnection of the two systems.
- *Services Offered.* Describe the nature of the information services (e.g. e-mail, FTP, database query, file query, general computational services) offered over the interconnected system by each participating organization.
- *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.
- *User Community.* Enter a thorough explanation of the “user community” who 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.
- *Information Exchange Security.* Enter a description of all system security technical services pertinent to the secure exchange of data among and between the systems in question.
- *Rules of Behavior.* Summarize the aspects of behavior 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 that provides for defense against intrusion, tampering, and virus detection, among others. Do not enter statements of law or policy. Such statements typically are addressed in the MOU/A.

- *Formal Security Policy.* Enter the titles of the formal security policy(ies) that govern each system. For example, “Information Systems Policy And Procedures, Number xxxx” for (name of Organization A).
- *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 its own (procedure name) procedures.” If no incident reporting is being performed, so state.
- *Audit Trail Responsibilities.* Describe how the audit trail responsibility is to be shared by participating organizations and what events each should be logged by each organization. If no audit trail is performed, so state.

OPTIONAL ITEMS: (Do not include this title “Optional Items” in the ISA.) If the technical representatives determine that any item below is “not applicable,” a statement to that effect may be made in the ISA in lieu of eliminating the item from the ISA. For example, if there is no dialup connectivity, the appropriate entry would be “Dialup capability will not be used by either interconnected system.”

- *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 being requested are 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, then 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 awareness, training requirements, and the assignment of responsibility for conducting it 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 Connectivity.* Describe any special considerations for dialup connections via public switched telephone network (PSTN) to any system in the proposed interconnection, including additional security risks and any safeguards to mitigate them.

- *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.

A.8 SECTION 3: TOPOLOGICAL DRAWING

The ISA should include a topological drawing depicting the interconnectivity from end-point to end-point. The drawing should include the following:

- The title “SECTION 3: TOPOLOGICAL DRAWING.”
- All communications paths, circuits, and other components used for the interconnection, beginning with the Organization A-owned system(s) traversing through all interconnected systems to the Organization B end-point.
- The drawing should depict the logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations).
- Center the words “FOR OFFICIAL USE ONLY” as the last line on the bottom of the page containing the drawing.

A.9 SECTION 4: SIGNATORY AUTHORITY

The ISA should include a signature conclusion. Optionally, this section may include any statements that the two DAAs desire in order to finalize the ISA. The signature conclusion should include the following:

- The expiration date of the agreement.
- Periodic review requirements, such as the date of the next review. If none is required, so state.
- Other statements as required by the DAAs, if any.
- The signatures of the DAAs from each organization, and the date of the signatures.

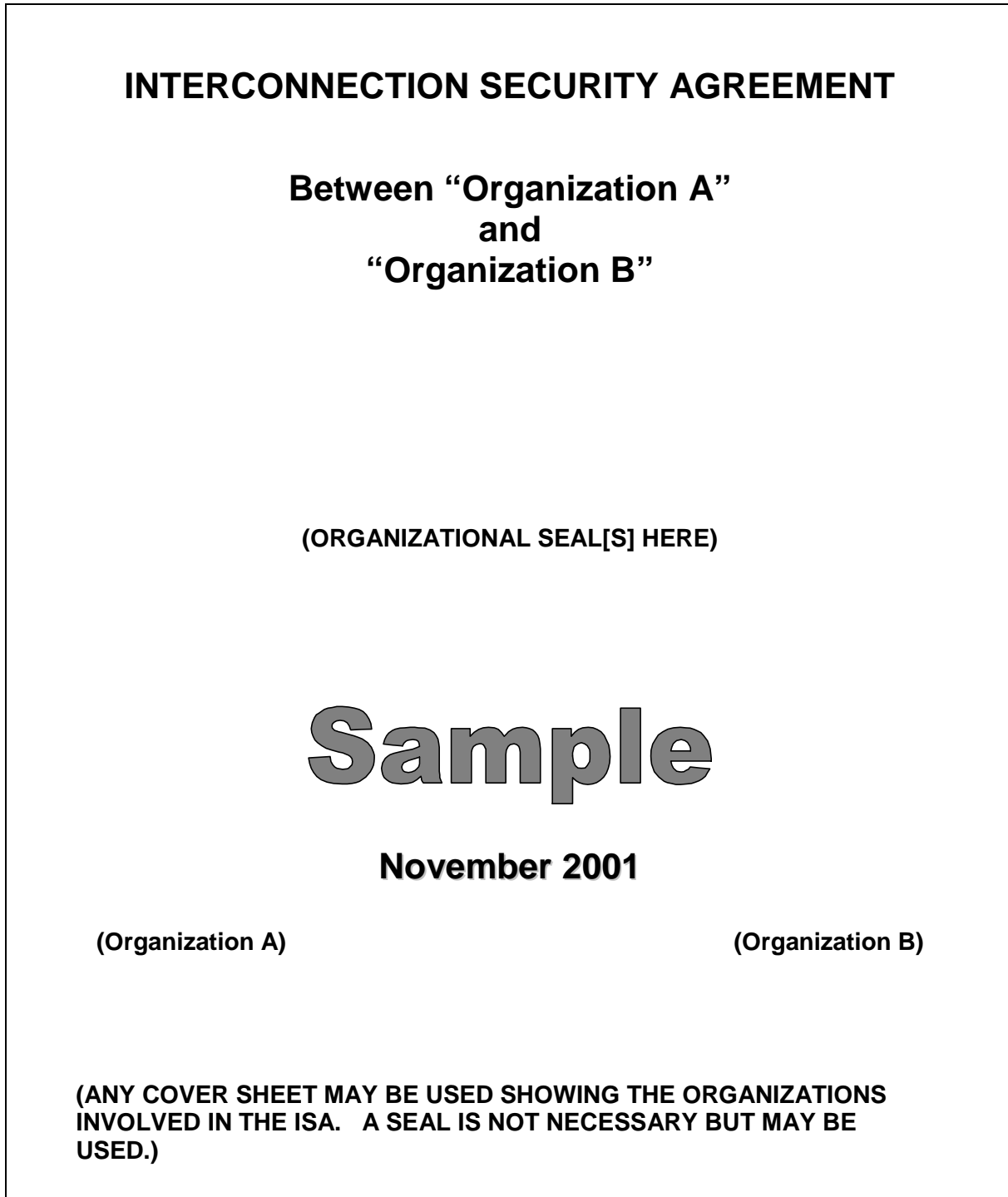


Figure A-1. ISA Sample

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 passing data from "System A," owned by "Organization A," to "System B" owned by "Organization B." "Organization B" requires the use of "Organizations A's" XYZ database as approved and directed by the Secretary of "Agency" in "Proclamation A," dated "date." The expected benefit is to (describe the expected benefit).

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 one-way path designed expressly for the delivery of the "XYZ database" to "Organization B's" Data Analysis Department. The information gained from the "XYZ database" will be fused with other information gained by internal "Organization B" resources.
- **Services Offered.** No user services are offered. This connection only passes data from the "Organization A" system to the "Organization B" system via a dedicated in-house connection. No data except control signals will be sent from "System B" to "System A."
- **Data Sensitivity.** The sensitivity of the data from "Organization A" is *Sensitive-But-Unclassified*. No data is sent from "Organization B" to "Organization A."
- **User Community.** All "Organization B" users with access to the data are U.S. citizens with a valid and current "Organization B" background Investigation.
- **Information Exchange Security.** The security of the information being passed on this one-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. Once the data has been stored on "System B," all access is controlled by authentication methods to validate the approved users.

Figure A-1. Continued

APPENDIX B MEMORANDUM OF UNDERSTANDING/AGREEMENT

The organizations that own and operate the connected systems should establish a Memorandum of Understanding (or Agreement) (MOU/A) that defines the responsibilities of both parties in establishing, operating, and securing the interconnection. This management document should not contain technical details of the interconnection. Those details should be addressed separately in the Interconnection Security Agreement (ISA) (see Appendix A).

An MOU/A should be developed and signed during the planning phase of the interconnection. Just prior to the activation of the interconnection, the memorandum should be reviewed, modified if necessary, and resigned.

An MOU/A development guide is provided below, although organizations may use their own MOU/A format, if appropriate. Figure B-1 depicts a sample MOU/A.

B.1 SUPERSESSION

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

B.2 INTRODUCTION

Use this section to describe the purpose of the memorandum. Sample language is provided in the sample memorandum. Identify the organizations and information systems that are involved in the interconnection.

B.3 AUTHORITIES

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

B.4 BACKGROUND

Use this section to describe the information systems that will be connected; the data that will be shared, exchanged, or passed one way across the interconnection; and the business purpose for the interconnection.

The description of the systems should be brief and nontechnical. The goal is to identify the systems and their boundaries. The memorandum should not provide system specifications. This section should include the formal name of each system; briefly describe their functions; identify their physical locations; identify their sensitivity or classification level; and identify the type(s) of data they store, process, and/or transmit.

B.5 COMMUNICATIONS

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

B.6 INTERCONNECTING SECURITY AGREEMENT

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

B.7 SECURITY

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

B.8 COST CONSIDERATIONS

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

B.9 TIMELINE

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

B.10 SIGNATORY AUTHORITY

The memorandum must include a signature conclusion, containing two signature blocks for each designated approval authority. Place the two signature blocks on the same line: one signature on the left and one on the right. Include an area for the “date” signed.

**MEMORANDUM OF UNDERSTANDING
(OR AGREEMENT)**

**Between “Organization A”
and
“Organization B”**

(ORGANIZATIONAL SEAL[S] HERE)

Sample

November 2001

(Organization A)

(Organization B)

**(ANY COVER SHEET MAY BE USED SHOWING THE ORGANIZATIONS
INVOLVED IN THE ISA. A SEAL IS NOT NECESSARY BUT MAY BE
USED.)**

Figure B-1. MOU/A Sample

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" and "System 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 systems to pass data from "System A" to "System B." Organization B requires the use of "Organization B's" "XYZ database" as approved and directed by the Secretary of "Agency" in "Proclamation A." The expected benefit of the interconnection is to (describe the expected benefit).

Each information 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

Figure B-1. Continued

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" 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 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 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 resign the ISA within one (1) month of implementation.
- **New Interconnections:** The system owner will be notified within one (1) month *before* the initiating party connects its information system with any other information 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 the system owner or technical lead. In addition, both parties will provide notification of any changes in point of contact information.

Figure B-1. Continued

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. The ISA will be renegotiated before changes are implemented. 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.

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 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)

(Date)

(Signature)

(Date)

Figure B-1 – Continued.

APPENDIX C

SYSTEM INTERCONNECTION IMPLEMENTATION PLAN

Appendix C provides guidance on developing a System Interconnection Implementation Plan, and is based on the discussion in Section 4. In addition, refer to NIST Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, for guidance on security principles that should be incorporated into planning activities.

C.1 INTRODUCTION

Describe the purpose and scope of the implementation plan, and identify policy requirements or guidance on which the system interconnection is based. Identify the information systems that will be interconnected, the organizations that own them, and the purpose for which they are used. Discuss the purpose for interconnecting the systems, and describe the services that will be offered over the interconnection. Briefly describe each section of the document.

C.2 SYSTEM INTERCONNECTION DESCRIPTION

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

C.2.1 Security Controls

Identify and describe the security controls that are currently in place for the information systems that will be interconnected. Identify the threats that could compromise the system interconnection, and describe how existing security controls will be configured to mitigate those threats. Identify any new security controls that will be implemented, including network- and application-level controls.

C.2.2 System Hardware

Hardware is the physical equipment associated with an information system. Identify and describe the hardware that is currently used on the systems that will be interconnected, and describe how it will support the interconnection. Identify and describe any new hardware that will be installed as part of the interconnection, including its function.

C.2.3 System Software

Software includes the application programs, software routines, and operating system software associated with an information system. Identify and describe software currently used on the systems that will be interconnected, and describe how it will be used to support the interconnection. Identify any new software that will be installed as part of the interconnection, including its function.

C.2.4 Data/Information Exchange

Organizations connect information systems to share data, make data available, or pass data one way from one organization to the other. It may be necessary to install a database that is dedicated to the interconnection. Identify the type(s) of data that will be exchanged between the organizations, and describe the transmission methods that will be used. Identify how the data will be stored and processed. Provide a data flow diagram.

C.2.5 Services and Applications

Describe the services and applications that the participating organizations will provide over the interconnection, as well as any new services or applications that will be developed, both initially and in the future. Examples include e-mail, database query, file query, and general computational services, application servers, and authentication servers.

C.3 ROLES AND RESPONSIBILITIES

Identify the personnel who will establish and maintain the system interconnection, and define their respective roles and responsibilities. A variety of staff skills may be required, including a program manager, network architect, security specialist, system administrator, network administrator, database administrator, application developer, and graphics designer. Staff from both organizations should be involved, if appropriate. Also, identify the responsibilities of staff who will use the interconnection after it is established (i.e., the users). The interconnection rules of behavior should be consulted when developing this section.

C.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 suggested tasks is provided below. Organizations should view them in the context of their own requirements. In addition, provide a checklist for each task to ensure it is performed properly.

C.4.1 Implement Security Controls

The process of interconnecting information systems could open an organization to a range of security vulnerabilities. Consequently, the first step that organizations should take is to implement appropriate security controls. Provide procedures for configuring current controls and, if necessary, implementing new controls. Security controls may include firewalls, identification and authentication mechanisms, logical access controls, encryption devices, intrusion detection systems, and physical security measures.

C.4.2 Install Hardware and Software

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

C.4.3 Develop and Install Applications

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

C.4.4 Conduct Operational and Security Testing

Provide detailed test procedures to verify whether the interconnection operates efficiently and securely. Also, describe how the results of the testing will be measured, and how deficiencies will be addressed.

C.4.5 Conduct a Risk Assessment

Describe the process for conducting an assessment to identify risks associated with the newly established interconnection, or refer to an organization's existing risk assessment methodology. Discuss how risks will be addressed. For example, risks may be mitigated by adjusting security controls or by implementing additional countermeasures.

C.4.6 Provide Training and Security Awareness

Describe a training and awareness program to train all personnel who are involved in the management, use, and operation of the system interconnection, including any new computer applications associated with it. Training should ensure that all staff know the rules of behavior associated with the interconnection and how to request assistance if they encounter problems. In addition, personnel who are responsible for maintaining the interconnection should receive specialized training to ensure they are proficient in their responsibilities.

C.5 SCHEDULE AND BUDGET

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

APPENDIX D REFERENCES

Christopher King, “Extranet Access Control Issues,” in Harold F. Tipton and Micki Krause, ed., *Information Security Management Handbook*, Vol. 2, 4th edition (New York: Auerbach, 2000), 99-114.

Defense Authorization Act (Fiscal Year 2001) (Public Law 106-398), Title X, Subtitle G, *Government Information Security Reform*, October 30, 2000.

Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, December 26, 1985.

Department of Health and Human Services, *Automated Information Systems Security Program Handbook* (<http://irm.cit.nih.gov/policy/aissp.html>).

“Federal Reserve: Sound Practices Guidance on Information Security,” *Computer Security Journal*, Vol. XIV, No.1, 1998, 45-68.

Herold, Rebecca and Slemo Warigon, “Extranet Audit and Security,” *Computer Security Journal*, Vol. XIV, No. 1, 1998, 35-44.

GartnerGroup, “Extranet Security: Five Ways to Manage High-Stakes Risk,” Research Note, July 21, 1997.

GartnerGroup, “Securing the Extranet: A Statement of Understanding,” Research Note, January 20, 1998.

National Institute of Technology and Standards, Federal Information Processing Standards (FIPS) 186-2, *Digital Signature Standard (DSS)*, January 2000.

National Institute of Technology and Standards, Special Publication 800-3, *Establishing a Computer Security Incidence Response Capability*, November 1991.

National Institute of Technology and Standards, Special Publication 800-9, *Good Security Practices for Electronic Commerce, Including Electronic Data Interchange*, December 1993.

National Institute of Technology and Standards, Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

National Institute of Technology and Standards, Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

National Institute of Technology and Standards, Special Publication 800-18, *Guide for Developing Security Plans and Information Technology Systems*, December 1998.

National Institute of Technology and Standards, Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, August 2001.

National Institute of Technology and Standards, Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2001.

National Institute of Technology and Standards Special Publication 800-31, *Intrusion Detection Systems*, August 2001.

Norman E. Smith, “Extranet Planning Guide,” September 27, 1999.
(<http://itmanagement.earthweb.com>).

Office of Management and Budget (OMB), Circular A-130, *Management of Federal Information Resources, Security of Federal Automated Information Resources, Appendix III*, November 2000.

Online Source, “Establishing an Extranet: Overview” (www.office.com/global).

Public Law 100-235, *Computer Security Act of 1987*, January 8, 1988.

Solutionary, “How to Protect Information: A Comprehensive Guide to Securing Networks and Systems,” 2001 (www.solutionary.com).

U.S. Customs Service, “Interconnection Security Agreements,” August 25, 2000
(www.bsp.gsa.gov/list.cfm).