UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

MIGRATION PLANNING GUIDANCE DELIVERABLES

INTERCONNECTION SECURITY AGREEMENT TEMPLATE

May 23, 2008

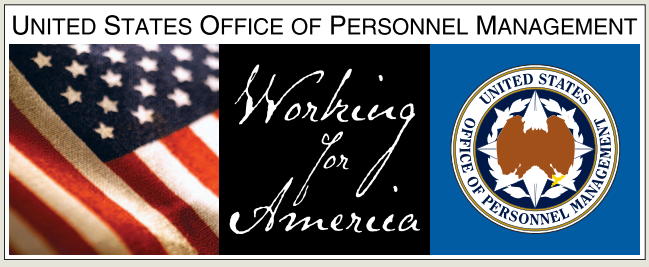

Table Of Contents

1. Overview

The purpose of the overview section is to describe the agreement between the Customer Agency and Shared Service Center and connectivity protocols. The information presented within the Interconnection Security Agreement (ISA) 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 for the two Designated Approval Authorities to make a prudent decision on approving the interconnection. This section should be tailored to the Customer Agency's network connection requirements.

The [CUSTOMER AGENCY] and the [SHARED SERVICE CENTER] agree to connect their networks for the purpose of providing system users, located within the [CUSTOMER AGENCY], access to [SHARED SERVICE CENTER]-based applications. The approach outlined in this agreement is intended to provide the [CUSTOMER AGENCY] with a network solution that provides capabilities designed to maximize the availability and reliability of applications services to the [CUSTOMER AGENCY]. The interconnection agreement includes:

- One primary network connection to the [SHARED SERVICE CENTER] SYSTEM in CITY and STATE.
- A backup dial-up connection.
- Two primary network connections to the [SHARED SERVICE CENTER] SYSTEM in CITY, STATE. These have been established at the [CUSTOMER AGENCY] primary site and [CUSTOMER AGENCY] COOP site.
- A backup connectivity method for use in the event of the loss of primary connectivity from only the [CUSTOMER AGENCY] primary site.
- Additional network connections to the [SHARED SERVICE CENTER] SYSTEM Business Continuity Recovery Site only from the [CUSTOMER AGENCY] primary site.
- Alternate remote connectivity capabilities the [CUSTOMER AGENCY] may use in meeting the organization’s needs.

All connectivity entering the [SHARED SERVICE CENTER] network will possess a source Internet Protocol (IP) (TCP/IP) address range that:

1. is an American Registry of Internet Numbers (ARIN) registered address; and,
2. is registered to the customer.

The IP address will be registered to the customer or related to the customer by reference from the IP address owner. Connectivity entering the [SHARED SERVICE CENTER]’s network will pass through several layers of network and server-based controls including Intrusion Detection Systems (IDS), packet filtering systems, and proxy filtering systems, as appropriate. [Shared Service Center to update as necessary]

Additionally, all traffic that originated from the Internet (outside the customers internal network) is not permitted to the [SHARED SERVICE CENTER]'s network unless the customer has previously:

1. Encrypted from desktop to Customer perimeter using strong encryption methods (using a FIPS 140-2 cryptographic module).
2. Authenticated the connection using strong shared secret software token (twelve characters with mixed case and numbers).
3. Use of a secure web browser that accommodates Secure Socket Layer (SSL) with 1024 bit encryption.

The customer and provider agencies will target the use of two-factor authentication for administrative control of all routers and firewalls, as well as two-factor authentication for the connection from the customer agency LAN to the provider agency's production backbone.

(Attachment 1 of this agreement contains a mapping between NIST SP 800-47 requirements and the location of the information within the provided documentation.) *[Both the Shared Service Center and Customer Agency will need to update this attachment]*

2. System Security Considerations

2. 1 General Information / Data Description

The purpose of this section is to describe the system security considerations for both the Customer Agency and Shared Service Center systems and applications.

[CUSTOMER AGENCY] uses # core applications hosted at the [SHARED SERVICE CENTER].

- [SHARED SERVICE CENTER HUMAN RESOURCES SYSTEM]

The Federal Human Resources and Privacy Act data traversing this interconnection is classified as [CATEGORIZATION TITLE]. Both [SHARED SERVICE CENTER] and [CUSTOMER AGENCY] must protect the data against disclosure, corruption, and unavailability. Data traversing this connection is not encrypted. The dedicated nature of the connection is sufficient to protect the data from unauthorized disclosure.

Due to the fact that the [SHARED SERVICE CENTER] systems are hosted and operated within the confines of the [SHARED SERVICE CENTER DATA CENTER], many of the physical, environmental, and logical security and access controls of the system are provided herein as a reference document to provide the ability to cross-check the types of protections and controls required for the [SHARED SERVICE CENTER SYSTEMS] Human Resources systems that are provided by the [SHARED SERVICE CENTER DATA CENTER]. The [SHARED SERVICE CENTER DATA CENTER] enclave received its Certification and Accreditation on XX-XX-XXXX. [*Shared Service Center to identify date that C&A was last completed]*

The [SHARED SERVICE CENTER] to [CUSTOMER AGENCY] connection will terminate at the following locations:

[CUSTOMER AGENCY]	[SHARED SERVICE CENTER]
STREET NAME	STREET NAME
CITY, STATE, ZIP CODE	CITY, STATE, ZIP CODE

2. 2 [SHARED SERVICE CENTER DATA CENTER] Description

The purpose of this section is to describe the Shared Service Center's data center. Following below is suggested language that can be modified according to the unique description of the Shared Service Center's data center.

The [SHARED SERVICE CENTER] is an OMB-designated franchising provider of automated human resources services and Data Center processing services. The [SHARED SERVICE CENTER] is a [BUSINESS MODEL, i.e. fee-for-service] organization providing human resources computing services for X Federal agencies with approximately X clients. *[Shared Service Center to provide information on number of Federal agencies and clients for which the system manages data]* The [SHARED SERVICE CENTER] SYSTEM provides customer support X hours per day, X days per week.

The [SHARED SERVICE CENTER DATA CENTER] is a [ENTER SYSTEM TYPE] system. The [SHARED SERVICE CENTER DIVISION] is responsible for managing the [SHARED SERVICE CENTER DATA CENTER SYSTEM TYPE] in support of [SHARED SERVICE CENTER] clients and a variety of sponsored applications. Direct computer services are also provided to many clients in support of their specific applications.

Location: [SHARED SERVICE CENTER]
STREET NAME
CITY, STATE ZIP CODE

[SHARED SERVICE CENTER DATA CENTER] description of data, including sensitivity or classification level: Federal Human Resources and Privacy Act data is stored, processed and transmitted from the [SHARED SERVICE CENTER DATA CENTER]. Though the data categorization is [CATEGORIZATION TITLE], its sensitivity demands strong measures to provide a high level of confidence that its confidentiality, integrity, and availability are preserved. Personal Identifiable Information (PII), be it citizen or government employee PII, raises the default confidentiality level to at least moderate. PII is information that actually identifies people or businesses. Examples include direct references such as name, address, social security number, employer identification number, or other identifying number or code such as

telephone number or email address. It also includes any information used separately or in combination to reference other data elements that are used for identification such as gender, race, date of birth, or geographic indicator. PII may be either citizen or government employee information. Privacy Impact Assessments are required by the E-Government Act of 2002, and must be conducted on every program that contains PII.

The [SHARED SERVICE CENTER DATA CENTER]'s FIPS 199 categorization is [HIGH, MODERATE OR LOW]. The [SHARED SERVICE CENTER SYSTEM]'s high water mark for Confidentiality, Integrity, and Availability ratings are summarized as:

Applicable NIST 800-60 Information Types & SYSTEMs	C	I	A
FIPS 199 High Water Mark – [SHARED SERVICE CENTER DATA CENTER]			

2. 3 [SHARED SERVICE CENTER SYSTEM] Description

The purpose of this section is to describe the Shared Service Center's human resources system. Following below is suggested language that can be modified according to the unique system description of the Shared Service Center System.

The [SHARED SERVICE CENTER HUMAN RESOURCES SYSTEM] is a modern, on-line, and real-time human resources system, providing human resources management support to numerous Federal Government agencies, servicing more than # individual accounts. The [SHARED SERVICE CENTER HUMAN RESOURCES SYSTEM] handles all [HR TRANSACTIONS]. *[Please describe the scope and nature of HR transactions administrated by the system]*. [SHARED SERVICE CENTER HUMAN RESOURCES SYSTEM] is the [CUSTOMER AGENCY]'s human resources management system of record.

[CUSTOMER AGENCY] users of [SHARED SERVICE CENTER] applications must use a userID/password combination to access all applications. The [SHARED SERVICE CENTER] to [CUSTOMER AGENCY] connection is a direct point-to-point link on a private network connection. [CUSTOMER AGENCY] will follow the encryption guidelines the [CUSTOMER AGENCY] recommends for external connections to their Intranet.

[The Advanced Encryption Algorithm (AES) and the Triple Data Encryption Algorithm (TDEA) are currently the only algorithms approved for data encryption. Whenever AES is used, it shall be used as specified in FIPS 197; whenever TDEA is used, it shall be used as specified in NIST SP 800-67. For "high" impact categorized systems and any systems containing privacy-act data, data encryption is required]

[SHARED SERVICE CENTER HUMAN RESOURCES SYSTEM] received its Certification and Accreditation on XX-XX-XXXX.

2. 4 Services Offered

The interconnection between [SHARED SERVICE CENTER] and [CUSTOMER AGENCY] is established for the sole purpose of sharing [SHARED SERVICE CENTER]-based applications only with [CUSTOMER AGENCY] users via a dedicated [CUSTOMER AGENCY] connection. *[The type and nature of services to be provided will be identified in this section]*

2. 5 Data Sensitivity

Federal Human Resources and Privacy Act data traverse this connection. Though the data categorization is [CATEGORIZATION TITLE], its sensitivity demands strong measures to provide a high level of confidence that its confidentiality, integrity, and availability are preserved. For example:

- Confidentiality: Human Resources and personal information that traverses this interconnection must not be revealed to unauthorized persons. *[Provider and/or Customer Agency to provide example(s) of negative impact from disclosure of information]*
- Integrity: Changes to the data that traverses this interconnection could cause misreporting and [EXAMPLE]. *[Provider and/or Customer Agency to provide example(s) of negative impact from changes to data that traverse the connection]*
- Availability: Data that crosses this interconnection is critical to the timely completion of [SHARED SERVICE CENTER] Human Resources missions, such as [EXAMPLE]. *[Shared Service Center and/or Customer Agency to provide example(s) of negative impact from unavailability of system or information]*

2. 6 User Community

Access to [SHARED SERVICE CENTER] applications must be authorized by [CUSTOMER AGENCY] and must be necessary for the potential user to carry out assigned job functions. Privileges granted for that purpose must comply with the principles of separation of duties and of least privilege as stated in the *[SHARED SERVICE CENTER] Security Plan*(s). A potential user has **no** access to [SHARED SERVICE CENTER] resources or applications unless authorized by the owner of the resource or application and the user has only as much access privilege as is needed to perform the assigned tasks.

2. 7 Information Exchange Security

This section contains available communications protocols, data transfer capabilities, specific communications hardware, and encryption requirements to establish a secure connection to [SHARED SERVICE CENTER]. In addition, customers are required to connect to the [SHARED SERVICE CENTER] Human Resources system's primary and backup sites to maintain an availability that is higher than with only a single connection.

2. 8 Trusted Behavior Expectations / Rules of Behavior

The [SHARED SERVICE CENTER] and [CUSTOMER AGENCY] users are expected to protect data in accordance with the policies and standards of the Privacy Act, OMB A-130, [SHARED SERVICE CENTER], and [CUSTOMER AGENCY]. [SHARED SERVICE CENTER] users that access [SHARED SERVICE CENTER] information resources are required to accept by signature the [SHARED SERVICE CENTER] Rules of Behavior. In addition, [CUSTOMER AGENCY] policy requires major applications have application-specific rules of behavior that must be accepted and signed by application users.

2. 9 Formal Security Policy and Standards

The Executive and Legislative branches, Federal departments and agencies issue the security policies, standards, and laws. This interconnection must comply with the following Federal requirements:

- Federal Information Security Management Act (FISMA) as part of the E-Government Act of 2002
- Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources
- NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology systems

[CUSTOMER AGENCY] Information Security Policies and Guidance applicable to [CUSTOMER AGENCY] interconnection include:

- [CUSTOMER AGENCY] Example
- [CUSTOMER AGENCY] Example
- [CUSTOMER AGENCY] Example

The [SHARED SERVICE CENTER BUSINESS UNIT] and this interconnection must comply with security policies and standards applicable to the [SHARED SERVICE CENTER]. [SHARED SERVICE CENTER] security policy and standards are reflected in:

- [SHARED SERVICE CENTER] Example
- [SHARED SERVICE CENTER] Example
- [SHARED SERVICE CENTER] Example

2. 10 Incident Reporting

The [SHARED SERVICE CENTER] or [CUSTOMER AGENCY], upon discovering a security incident, shall report it in accordance with its agency-specific incident reporting procedures and shall expeditiously notify the [SHARED SERVICE CENTER] Help Desk at (XXX) XXX-XXXX or (XXX) XXX-XXXX *[Shared Service Center to insert relevant phone numbers for Help Desk]*. [SHARED SERVICE CENTER] will follow Incident Response Procedures, currently based on the [SHARED SERVICE CENTER POLICY]. *[Shared Service Center to*

identify Incident Response Policy Name and Number. For example, "NBCM-CIO-6310-001, Computer Security Response Team Handbook, Version 2.1.0, January 11, 2005."]

[SHARED SERVICE CENTER] technical staff shall immediately notify the designated [CUSTOMER AGENCY] counterpart by telephone or e-mail when a security incident(s) is detected, in order that the counterpart may take steps to determine whether the system has been compromised and to take appropriate action. The [CUSTOMER AGENCY] technical staff shall immediately notify the [CUSTOMER AGENCY] Help Desk at (XXX) XXX-XXXX. The [CUSTOMER AGENCY] IT Security team shall investigate as necessary and coordinate remediation activities.

2. 11 Audit Trail Responsibilities

Both agencies are responsible for auditing application processes and user activities involving this interconnection. Activities that will be recorded include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit trails will be retained for a period agreed upon by both parties. [CUSTOMER AGENCY] will conduct annual reviews in conjunction with the [SHARED SERVICE CENTER] security staff.

3. Level and Method of Interconnect

Figure 1 illustrates the network connectivity package for access to the [SHARED SERVICE CENTER] Data Center resources. The connectivity package includes the following.

[Tailor to Customer Agency Network Connection]

- Primary Connectivity
- Disaster Recovery Site Connectivity

Connectivity between each organization shall be allowed from the customer's (application system users) internal desktop environment to the [SHARED SERVICE CENTER]'s internal application production environment. At the customer's discretion, connectivity can be enabled that will permit the [SHARED SERVICE CENTER]'s internal production environment to access the customer's internal production environment. The [SHARED SERVICE CENTER] will not allow internal [SHARED SERVICE CENTER] desktops to access customer organizations networks. Additionally, a customer's internal desktop network will not be permitted to access [SHARED SERVICE CENTER] internal desktops or to access to other customer networks.

Primary Connectivity — the [SHARED SERVICE CENTER] and [CUSTOMER AGENCY] have agreed to establish a LAN to LAN VPN as the Primary Connectivity. The [CUSTOMER AGENCY] circuit begins at the perimeter of the [CUSTOMER AGENCY] network also connects to a [SHARED SERVICE CENTER] provided router located in the [CUSTOMER AGENCY]'s network perimeter. The circuit is an ATM dual T1 circuit at 1,536 kbps.

[Provider and/or Customer Agency to input the relevant circuit data] This circuit is intended for the sole use of the [CUSTOMER AGENCY] in connecting to the [SHARED SERVICE CENTER].

Disaster Recovery Site Connectivity — it is also agreed the [SHARED SERVICE CENTER] telecommunications staff have implement a method to access to the [SHARED SERVICE CENTER] Business Continuity and Recovery Center (BCRS), as a contingency in the event there is a disaster that renders the [SHARED SERVICE CENTER SYSTEM] unusable to meet [CUSTOMER AGENCY]'s business requirements. The circuit to the BCRS disaster recovery site is an ATM connection operating at 64 kbps. *[Provider and/or Customer Agency to input the relevant connection speed]*

Note: Access to internal customer networks from any [SHARED SERVICE CENTER]-based remote access method is not permitted.

Note: Satellite-based Internet connectivity is not supported.

4. Impact on Existing Infrastructure and Operations

There is no impact on the [SHARED SERVICE CENTER]'s existing infrastructure and operations as a result of this network interconnection. The network was designed to support multiple connections of this type.

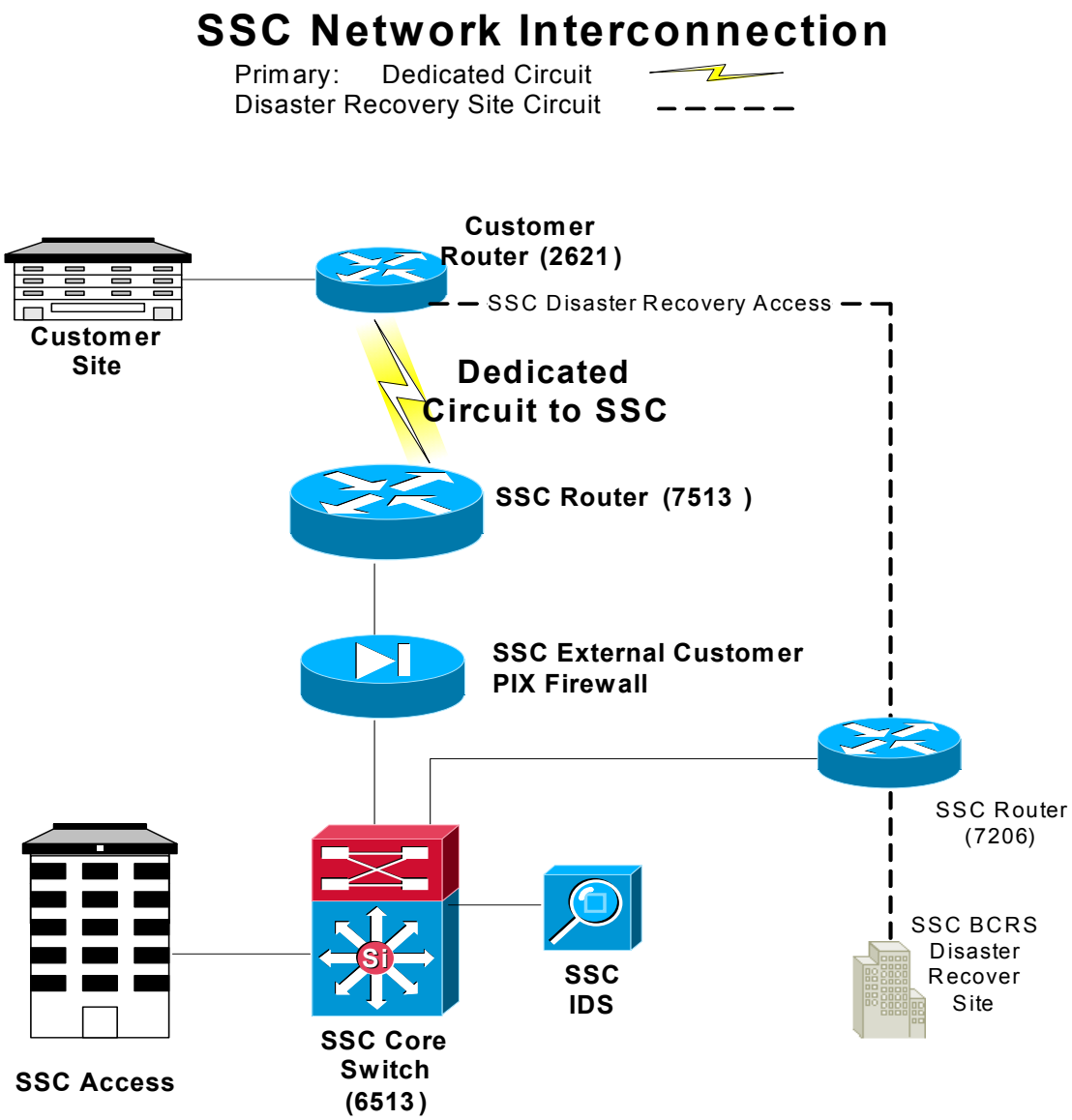

Figure 1. — High Level Diagram of [CUSTOMER AGENCY]/[SHARED SERVICE CENTER] Connectivity

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

- *Communications paths, circuits, and other components used for the interconnection, from "Organization A's" system to "Organization B's" system.*

- *The drawing should depict the logical location of components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations).]*

5. Hardware

The hardware used to support the connectivity is listed in Figure 1 of this document. No new hardware is required at the [SHARED SERVICE CENTER] SYSTEM to support this connectivity.

6. Software

The equipment supporting connectivity between the [CUSTOMER AGENCY] network and the [SHARED SERVICE CENTER]'s network will be operated and maintained by the [CUSTOMER AGENCY]'s technical staff as defined in the Roles and Responsibilities component of this document. The [SOFTWARE] levels will be maintained and kept current (current maintained production release as defined by the hardware vendor.) Patches will be applied for the [SOFTWARE] for the hardware, as vulnerabilities and "fixes" are made available and commensurate with the risk associated with the vulnerability. Access Control Lists (ACL's), the Firewall Feature Set, and other security controls will be fully implemented before production traffic is allowed to traverse the connection and as customer requirements and risks dictate.

Note: The [SHARED SERVICE CENTER] will not allow traffic from one [SHARED SERVICE CENTER] Customer to be routed through this network and into another [SHARED SERVICE CENTER] Customer's network. All outside requests for Customer data will be directed back to the Customer.

7. Roles and Responsibilities

[CUSTOMER AGENCY] technical staff up to the point of demarcation manages the network interconnection between [CUSTOMER AGENCY]'s network and the [SHARED SERVICE CENTER]'s internal network. The specifics of this agreement are delineated below.

Network Management — Management of the interconnection between the two organizations is performed from the two following perspectives:

1. Emergency or fault management
2. On-going operational support management (monitoring)

[Specify relevant network management applicable to your ISA]

Fault management will be undertaken by the organization primarily responsible for managing the interconnection ([SHARED SERVICE CENTER]). It is the responsibility of the managing organization to resolve the fault as expeditiously as possible, to communicate status of the

connectivity to organizational management, and to facilitate the communications between vendors and other technical personnel.

On-going operational management support shall also be the responsibility of the organization primarily responsible for the connectivity ([SHARED SERVICE CENTER]). The organization primarily responsible for the connectivity will be responsible for:

- Change and configuration management
- On-going bandwidth utilization monitoring

The [SHARED SERVICE CENTER] technical staff will manage the configuration of the hardware and software in accordance with the [SHARED SERVICE CENTER]'s Change Management processes and procedures (provided by [SHARED SERVICE CENTER]). Software configuration changes will be enacted after change requests are received and signed by the management of the interconnected organizations on appropriate request forms.

Table **7.1** for the appropriate management signatory levels required for network change and configuration management requests at the [SHARED SERVICE CENTER].

Table 7.1 — [SHARED SERVICE CENTER] IT Management Staff with Roles and Responsibilities

Organization	Name	Responsibilities
[SHARED SERVICE CENTER] CIO and Assistant Director, Information Technology Directorate	Name Address Phone Email address	Responsible for all IT Directorate activities. Authorizes emergency connectivity requirements using non-standard connectivity methodologies.
[SHARED SERVICE CENTER], Chief, Enterprise Infrastructure Division	Name Address Phone Email address	Responsible for the delivery and implementation of all IT Services within the [SHARED SERVICE CENTER]. Authorizes non-standard connectivity methodologies.
[SHARED SERVICE CENTER], Chief Information Security Officer	Name Address Phone Email address	Responsible for IT Security Policy.
[SHARED SERVICE CENTER] Chief, Network Services Branch	Name Address Phone Email address	Responsible for [SHARED SERVICE CENTER] Data Wide Area Networking. Authorizes all requests for standard connectivity and recommends approval of all non-standard connectivity methods.

Organization	Name	Responsibilities
[SHARED SERVICE CENTER] Help Desk	Name Address Phone Email address	The [SHARED SERVICE CENTER] Data Center provides customer support 24 hours per day, 7 days per week. Customers who need to report a problem or obtain assistance should call.

Table 7.2 — [CUSTOMER AGENCY] IT Management Staff with Roles and Responsibilities

Organization	Name	Responsibilities
[CUSTOMER AGENCY] CIO	Name Address Phone Email address	Responsible for all IT Directorate activities. Authorizes emergency connectivity requirements using non-standard connectivity methodologies.
[CUSTOMER AGENCY] Deputy CIO	Name Address Phone Email address	
[CUSTOMER AGENCY] IT Security Officer	Name Address Phone Email address	Responsible for IT Security Policy.
[CUSTOMER AGENCY] Chief, Network Services Branch	Name Address Phone Email address	Responsible for [CUSTOMER AGENCY] Data Wide Area Networking. Authorizes all requests for standard connectivity and recommends approval of all non-standard connectivity methods.
[CUSTOMER AGENCY] Help Desk	Name Address Phone Email address	The [CUSTOMER AGENCY] Help Desk provides technical support for all IT related questions and register all issues and incidents, including security related events.

8. 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 this ISA. Each party certifies that its respective system is designed, managed, and operated in compliance with all relevant Federal laws, regulations, and policies. Interconnecting systems shall have undergone a Certification and Accreditation (C&A) process with associated memorandums that designate the systems as fully accredited. To achieve this may require mitigation actions on the part of the client system owners.

9. Schedule

This element is not applicable because the circuits have been in place (existing) for a number of years and no planned connectivity changes are anticipated.

10. Supplementary Documentation

There may be requirements for SSC-unique supporting documentation to be appended to this ISA.

11. Signatory Authority

This ISA is valid for three (3) years after the last date on any signature below. *[May be adjusted according to agreement needs]* At that time, it will be updated, reviewed, and reauthorized. Either party may terminate this agreement upon 30 days' advanced notice in writing or in the event of a security incident that necessitates an immediate response.

_____	_____
First Last Name	**First Last Name**
Chief Information Officer	**Chief Information Officer**
[CUSTOMER AGENCY]	**[SHARED SERVICE CENTER]**
Date:_____	**Date:**_____

Attachment 1

CUSTOMER AGENCY AND SHARED SERVICE CENTER need to enter their cross-references in columns 2 and 3 below

Mapping of NIST SP 800-47 Requirements within Exchanged Documentation

NIST 800-47 Requirement	[SHARED SERVICE CENTER] Document Location	[CUSTOMER AGENCY] Document Location
Level and Method of Interconnection		
Impact on Existing Infrastructure and Operations		
Hardware Requirements		
Software Requirements		
Data Sensitivity		
User Community		
Services and Applications		
Security Controls		
Segregation of Duties		
Incident Reporting and Response		
Contingency Planning		
Data Element Naming and Ownership		
Data Backup		
Change Management		
Rules of Behavior		
Security Training and Awareness		
Roles and Responsibilities		
Scheduling		
Costs and Budgeting		

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
1900 E Street, NW
Washington, DC 20415

HRLOB/ISAT052008