Interconnection Security Agreement

& Memorandum of Understanding

Between

[System A Name] &

[System B Name]

[Agency A]

[Agency B]

Revision: [??]

Date: [Month], [Year]

Document Information

|  |  |
| --- | --- |
| **[System A] Point of Contact** | |
| Name |  |
| Contact Number |  |
| E-mail Address |  |
| **[System B] Point of Contact** | |
| Name |  |
| Contact Number |  |
| E-mail Address |  |

| **Document Review** | | | |
| --- | --- | --- | --- |
| **System ISSPM Name** | **System ISSPM Signature** | **Date** | **Comments (if any)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| **Distribution List** | | | |
| --- | --- | --- | --- |
| **Name** | **Title** | **Agency/Office** | **Contact Information** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Interconnection Security Agreement Authorization

We have carefully reviewed the Interconnection Security Agreement (ISA) between [System A Name (System Acronym)] and [System B Name (System Acronym)]. This document has been completed in accordance with the requirements set forth in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*. This agreement will be reviewed annually on the previous page and will be re-signed by all parties every third year.

[System A Name (System Acronym)]

NAME DATE  
Information System Owner

NAME DATE  
[Agency] Information System Security Manager

NAME DATE  
[System] Authorizing Official

-----------------------------------------------------------------------------------------------------------

[System B Name (System Acronym)]

NAME DATE  
Information System Owner

NAME DATE  
[Agency] Information System Security Manager

NAME DATE  
[System] Authorizing Official

**Table of Contents**

[Document Information ii](#_Toc291081091)

[Interconnection Security Agreement Authorization iii](#_Toc291081092)

[1 Introduction 1](#_Toc291081093)

[2 Connection Purpose 1](#_Toc291081094)

[2.1 System Identification 1](#_Toc291081095)

[2.2 Connection Purpose and Information Shared/Passed 2](#_Toc291081096)

[2.3 Information Sensitivity 2](#_Toc291081097)

[3 Connection Specifics 2](#_Toc291081098)

[3.1 Connection Method 2](#_Toc291081099)

[3.2 Connection Segregation 2](#_Toc291081100)

[4 System Vulnerabilities 2](#_Toc291081101)

[5 Common/Hybrid Controls 2](#_Toc291081102)

[6 Incident Reporting 3](#_Toc291081103)

[7 Backups/Updates/Changes 3](#_Toc291081104)

[8 User Community 3](#_Toc291081105)

[9 Rules of Behavior 3](#_Toc291081106)

[10 NIST SP 800-53 Rev 3 Controls 3](#_Toc291081107)

[11 Cost Considerations 4](#_Toc291081108)

[12 Audit Trail Responsibilities 4](#_Toc291081109)

[13 Topological/Informational Flow Drawing 4](#_Toc291081110)

[14 Timeline 4](#_Toc291081111)

[Appendix A. [System A Name] Plan of Action and Milestones 1](#_Toc291081112)

[Appendix B. [System B Name] Plan of Action and Milestones 1](#_Toc291081113)

[Appendix C. Inherited controls 1](#_Toc291081114)

***NOTE TO AUTHOR****: Highlighted, italicized text throughout this template is provided solely to assist you in creating this document. Please delete all such text prior to submitting this document. In addition, replace all items enclosed in square brackets [ ] with actual information and remove the highlighting.*

# Introduction

A system interconnection is defined as the direct connection of two or more information technology (IT) systems for the purpose of sharing data and other information resources. The NIST SP 800-53 (Revision 3) Certification and Accreditation - Control 3 (CA-3) primarily refers to connections but uses the terms connections and interconnections interchangeably. An interconnection security agreement (ISA) is used to document connections between systems. The ISA is much more than a contract or service agreement between two agencies/departments/divisions; the ISA is a security agreement that protects both interconnected systems from each other. The intent behind an ISA is to detail some basic system information and then to document and agree on how the security of the two systems will be maintained. Significant benefits that can be realized through a system connection include: reduced operating costs, greater functionality, improved efficiency, and centralized access to data. Interconnecting IT systems may also strengthen ties among participating organizations by promoting communication and cooperation.

# Connection Purpose

*In this section document the purpose of interconnecting the two systems. What information is shared? What is the sensitivity of the information shared?*

## System Identification

**System A:**

[Department, Agency, Division, System Name (System Acronym)]

FIPS 199 Categorization: [Low, Moderate or High]

Authority to Operate (ATO) Date: [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]

System Owner Name: [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]

Contact Number: [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]

Email Address: [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]

**System B:**

[Department, Agency, Division, System Name (System Acronym)]

FIPS 199 Categorization: [Low, Moderate or High]

Authority to Operate (ATO) Date: [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]

System Owner Name: [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]

Contact Number: [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]

Email Address: [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]

## Connection Purpose and Information Shared/Passed

*Describe the purpose of the interconnection. If the purpose is to provide connectivity (such as an application residing on a general support system (GSS) then explain that. If the connection purpose is to share or pass information, generally what information is passed? Is the information PII and if so, exactly what PII is passed. .*

## Information Sensitivity

*Describe the sensitive nature of the information. If there is privacy data on the system, please make sure that is identified in Section 2.2.*

# Connection Specifics

## Connection Method

*How are the two systems connected? Direct connect? Virtual Private Network? Over the Internet? FIPS-140-2 compliant encryption?*

## Connection Segregation

*If the two systems being connected have different FIPS 199 categorizations, how are the systems going to be segregated to ensure that a vulnerability that could be exploited on the lower categorized system cannot be used to compromise the higher categorized system..*

# System Vulnerabilities

One system's vulnerabilities can have an adverse impact on the security of another system, especially when the two systems are connected and sharing information. Because of this, the system owners and the security officers must be aware of the identified vulnerabilities of all the systems that are connected to their system.

At the time of entering into this ISA, the current Plan of Action and Milestones (POA&M) for System A can be found in Appendix A. The POA&M for System B can be found in Appendix B. Special attention should be paid to any moderate or high vulnerabilities. With this in mind, the system owners of both systems agree that any new vulnerabilities categorized as moderate or higher risk will immediately be sent to the other system's owner/security officer.

# Common/Hybrid Controls

Some connected systems rely heavily on the other connected system for control implementations that are common across the two (or more) systems that are connected. This occurs often when an application resides on a GSS. The GSS provides a certain number of controls to all applications (and possibly other GSSs) that reside on it. For these circumstances, the owner of the system that is inheriting the controls specifies all the controls that are inherited from the other system in the template in Appendix C. Note that the template also contains hybrid controls where the common portion of the control is provided by the GSS. For systems that just share data, this section and the appendix are not applicable.

*The system owner of the system that is inheriting controls from the GSS, must check off all inherited/hybrid controls in Appendix C.*

# Incident Reporting

*Document the process each system owner will follow in the event of an incident.* (Ex: An incident identified with either system will immediately be reported to the other system's owner/security officer.)

# Backups/Updates/Changes

*Document who is responsible for performing backups of the data. Who must be notified if any changes are going to be made to either system? How significant does the change need to be to warrant such notification? What notification is required when maintenance will be performed on the system?*

# User Community

*Describe the “user community” that will be served by the interconnection, including their approved access levels and the lowest approval level of any individual who will have access to the interconnection. Also, discuss requirements for background investigations and security clearances, if appropriate.*

# Rules of Behavior

*Summarize the aspects of behavior expected from users who will have access to the interconnection. Each system is expected to protect information belonging to the other through the implementation of security controls that protect against intrusion, tampering, and viruses, among others. Do not enter statements of law or policy. If the systems are from different departments, consider appending both department's rules of behavior to this agreement.*

# Controls

*This section is for the documenting of any specific controls that must be maintained in order to ensure the connection is secure.*

.

# Cost Considerations

*Briefly describe any cost issues/considerations that need to be identified. If different departments/agencies are involved, or if the method of interconnection is expensive, the following example may be used:*

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.

# Audit Trail Responsibilities

*Describe how the audit trail responsibility will be shared by the organizations and what events each organization will log. Specify the length of time that audit logs will be retained. If no audit trail is performed, so state.*

# Topological/Informational Flow Drawing

*Provide a topological and/or information flow drawing that clearly shows the systems and their interconnection.*

# Timeline

This agreement will remain in effect for one (1) year after the last date on either Authorizing Official's signature. After one (1) year, this agreement can be continued for an additional two years with concurrence from the ISSPMs for the systems involved. If the parties wish to extend this agreement beyond the three years, 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 with 30 days advanced notice or in the event of a security incident that necessitates an immediate response.

1. [System A Name] Plan of Action and Milestones

Below is a complete listing of open items from this system's POA&M.

1. [System B Name] Plan of Action and Milestones

Below is a complete listing of open items from this system's POA&M.

1. Inherited controls

Below is a complete listing NIST SP 800-53 Rev. 3 Controls. Any controls inherited from the host system will be checked. Hybrid controls, due to their dual nature, are also listed. This listing helps the system owners by explicitly listing those controls that are specifically needed.

| ***FISMA Control  (NIST 800-53 Rev3)*** | | | ***NIST 800-53 Control Name*** |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Control | Enhance ment | Applicable FIPS 199 Baseline |  | **Common Controls** | **Hybrid Controls** | Notes |
| **Access Controls** | | | |  |  |  |
| AC-1 |  | L,M,H | Access Control Policy and Procedures |  |  |  |
| AC-2 |  | L,M,H | Account Management |  |  |  |
|  | AC-2(1) | M,H |  |  |  |  |
|  | AC-2(2) | M,H |  |  |  |  |
|  | AC-2(3) | M,H |  |  |  |  |
|  | AC-2(4) | M,H |  |  |  |  |
| AC-3 |  | L,M,H | Access Enforcement |  |  |  |
| AC-4 |  | M,H | Information Flow Enforcement |  |  |  |
| AC-5 |  | M,H | Separation of Duties |  |  |  |
| AC-6 |  | M,H | Least Privilege |  |  |  |
|  | AC-6(1) | M,H |  |  |  |  |
|  | AC-6(2) | M,H |  |  |  |  |
| AC-7 |  | L,M,H | Unsuccessful Login Attempts |  |  |  |
| AC-8 |  | L,M,H | System Use Notification |  |  |  |
| AC-9 |  | NS | Previous Logon (Access) Information |  |  | N/A - Not Selected |
| AC-10 |  | H | Concurrent Session Control |  |  |  |
| AC-11 |  | M,H | Session Lock |  |  |  |
| AC-12 |  |  | Session Termination |  |  | Withdrawn |
| AC-13 |  |  | Supervision and Review-Access Control |  |  | Withdrawn |
| AC-14 |  | L,M,H | Permitted Actions w/o Identification or Authentication |  |  |  |
|  | AC-14(1) | M,H |  |  |  |  |
| AC-15 |  |  | Automated Marking |  |  | Withdrawn |
| AC-16 |  | NS | Automated Labeling (Optional) |  |  | N/A - Not Selected |
| AC-17 |  | L,M,H | Remote Access |  |  |  |
|  | AC-17(1) | M,H |  |  |  |  |
|  | AC-17(2) | M,H |  |  |  |  |
|  | AC-17(3) | M,H |  |  |  |  |
|  | AC-17(4) | M,H |  |  |  |  |
|  | AC-17(5) | M,H |  |  |  |  |
|  | AC-17(6) | M,H |  |  |  |  |
|  | AC-17(7) | M,H |  |  |  |  |
|  | AC-17(8) | M,H |  |  |  |  |
| AC-18 |  | L,M,H | Wireless Access |  |  |  |
|  | AC-18(1) | M,H |  |  |  |  |
|  | AC-18(2) | H |  |  |  |  |
|  | AC-18(3) | H |  |  |  |  |
|  | AC-18(4) | H |  |  |  |  |
| AC-19 |  | L,M,H | Access Control for Mobile Devices |  |  |  |
|  | AC-19(1) | M,H |  |  |  |  |
|  | AC-19(3) | M,H |  |  |  |  |
|  | AC-19(1) | M,H |  |  |  |  |
| AC-20 |  | L,M,H | Use of External Information Systems |  |  |  |
|  | AC-20(1) | M,H |  |  |  |  |
| AC-21 |  | NS | User Based Collaboration and Information Sharing |  |  | N/A - Not Selected |
| AC-22 |  | L,M,H | Publically Accessible Content |  |  |  |
| **Awareness and Training** | | | |  |  |  |
| AT-1 |  | L,M,H | Security Awareness and Training Policy and Procedures |  |  |  |
| AT-2 |  | L,M,H | Security Awareness |  |  |  |
| AT-3 |  | L,M,H | Security Training |  |  |  |
| AT-4 |  | L,M,H | Security Training Records |  |  |  |
| AT-5 |  | NS | Contacts with Security Groups and Associations |  |  | N/A - Not Selected |
| Audit and Accountability | | | |  |  |  |
| AU-1 |  | L,M,H | Audit and Accountability Policy and Procedures |  |  |  |
| AU-2 |  | L,M,H | Auditable Events |  |  |  |
|  | AU-2(2) | M,H |  |  |  |  |
|  | AU-2(3) | M,H |  |  |  |  |
| AU-3 |  | L,M,H | Content of Audit Records |  |  |  |
|  | AU-3(1) | M,H |  |  |  |  |
|  | AU-3(2) | H |  |  |  |  |
| AU-4 |  | L,M,H | Audit Storage Capacity |  |  |  |
| AU-5 |  | L,M,H | Audit Processing |  |  |  |
|  | AU-5(1) | H |  |  |  |  |
|  | AU-5(2) | H |  |  |  |  |
| AU-6 |  | M,H | Audit Review, Analysis and Reporting |  |  |  |
|  | AU-6(1) | H |  |  |  |  |
| AU-7 |  | M,H | Audit Reduction and Report Generation |  |  |  |
|  | AU-7(1) | M,H |  |  |  |  |
| AU-8 |  | L,M,H | Time Stamps |  |  |  |
|  | AU-8(1) | M,H |  |  |  |  |
| AU-9 |  | L,M,H | Protection of Audit Information |  |  |  |
| AU-10 |  | NS | Non-repudiation |  |  |  |
| AU-11 |  | L,M,H | Audit Record Retention |  |  |  |
| AU-12 |  | L,M,H | Audit Generation |  |  |  |
|  | AU-12(1) | H |  |  |  |  |
| AU-13 |  |  | Monitoring for Information Disclosure |  |  | N/A - Not Selected |
| AU-14 |  |  | Session Audit |  |  | N/A - Not Selected |
| Certification, Accreditation, and Security Assessments | | | |  |  |  |
| CA-1 |  | L,M,H | Security Assessment and Authorization Policies and Procedures |  |  |  |
| CA-2 |  | L,M,H | Security Assessments |  |  |  |
|  | CA-2(1) |  |  |  |  |  |
|  | CA-2(2) |  |  |  |  |  |
| CA-3 |  | L,M,H | Information System Connections |  |  |  |
| CA-4 |  |  | Security Certification |  |  | Withdrawn |
| CA-5 |  | L,M,H | Plan of Action and Milestones |  |  |  |
| CA-6 |  | L,M,H | Security Accreditation |  |  |  |
| CA-7 |  | L,M,H | Continuous Monitoring |  |  |  |
| Configuration Management | | | |  |  |  |
| CM-1 |  | L,M,H | Configuration Management Policy and Procedures |  |  |  |
| CM-2 |  | L,M,H | Baseline Configuration and System Component Inventory |  |  |  |
|  | CM-2(1) | M,H |  |  |  |  |
|  | CM-2(2) | H |  |  |  |  |
|  | CM-2(3) | M,H |  |  |  |  |
|  | CM-2(4) | M,H |  |  |  |  |
|  | CM-2(5) | H |  |  |  |  |
|  | CM-2(6) | H |  |  |  |  |
| CM-3 |  | M,H | Configuration Change Control |  |  |  |
|  | CM-3(1) | H |  |  |  |  |
|  | CM-3(2) | M,H |  |  |  |  |
| CM-4 |  | M,H | Security Impact Analysis |  |  |  |
|  | CM-4(1) |  |  |  |  |  |
| CM-5 |  | M,H | Access Restrictions for Change |  |  |  |
|  | CM-5(1) | H |  |  |  |  |
|  | CM-5(2) | H |  |  |  |  |
|  | CM-5(3) | H |  |  |  |  |
| CM-6 |  | L,M,H | Configuration Settings |  |  |  |
|  | CM-6(1) | H |  |  |  |  |
| CM-7 |  | M,H | Least Functionality |  |  |  |
|  | CM-7(1) | M,H |  |  |  |  |
|  | CM-7(2) | H |  |  |  |  |
| CM-8 |  | L,M,H | Information System Component Inventory |  |  |  |
|  | CM-8(1) | M,H |  |  |  |  |
|  | CM-8(2) | H |  |  |  |  |
| CM-9 |  | M,H | Configuration Management Plan |  |  |  |
| Contingency Planning | | | |  |  |  |
| CP-1 |  | L,M,H | Contingency Planning Policy and Procedures |  |  |  |
| CP-2 |  | L,M,H | Contingency Plan |  |  |  |
|  | CP-2(1) | M,H |  |  |  |  |
|  | CP-2(2) | H |  |  |  |  |
|  | CP-2(3) | H |  |  |  |  |
| CP-3 |  | L,M,H | Contingency Training |  |  |  |
|  | CP-3(1) | H |  |  |  |  |
| CP-4 |  | L,M,H | Contingency Plan Testing |  |  |  |
|  | CP-4(1) | M,H |  |  |  |  |
|  | CP-4(2) | H |  |  |  |  |
|  | CP-4(4) | H |  |  |  |  |
| CP-5 |  |  | Contingency Plan Update |  |  | Withdrawn |
| CP-6 |  | M,H | Alternate Storage Sites |  |  |  |
|  | CP-6(1) | M,H |  |  |  |  |
|  | CP-6(2) | H |  |  |  |  |
|  | CP-6(3) | M,H |  |  |  |  |
| CP-7 |  | L,M,H | Alternate Processing Sites |  |  |  |
|  | CP-7(1) | M,H |  |  |  |  |
|  | CP-7(2) | M,H |  |  |  |  |
|  | CP-7(3) | M,H |  |  |  |  |
|  | CP-7(4) | H |  |  |  |  |
|  | CP-7(5) | M,H |  |  |  |  |
| CP-8 |  | M,H | Telecommunications Services |  |  |  |
|  | CP-8(1) | M,H |  |  |  |  |
|  | CP-8(2) | M,H |  |  |  |  |
|  | CP-8(3) | H |  |  |  |  |
|  | CP-8(4) | H |  |  |  |  |
| CP-9 |  | L,M,H | Information System Backup |  |  |  |
|  | CP-9(1) | M,H |  |  |  |  |
|  | CP-9(2) | H |  |  |  |  |
|  | CP-9(3) | H |  |  |  |  |
| CP-10 |  | L,M,H | Information System Recovery and Reconstitution |  |  |  |
|  | CP-10(2) | M,H |  |  |  |  |
|  | CP-10(3) | M,H |  |  |  |  |
|  | CP-10(4) | H |  |  |  |  |
| Identification and Authentication | | | |  |  |  |
| IA-1 |  | L,M,H | Identification and Authentication Policy and Procedures |  |  |  |
| IA-2 |  | L,M,H | User Identification and Authentication (Organizational Users) |  |  |  |
|  | IA-2(1) | L,M,H |  |  |  |  |
|  | IA-2(2) | M,H |  |  |  |  |
|  | IA-2(3) | M,H |  |  |  |  |
|  | IA-2(4) | H |  |  |  |  |
|  | IA-2(8) | M,H |  |  |  |  |
|  | IA-2(9\) | H |  |  |  |  |
| IA-3 |  | M,H | Device Identification and Authentication |  |  |  |
| IA-4 |  | L,M,H | Identifier Management |  |  |  |
| IA-5 |  | L,M,H | Authenticator Management |  |  |  |
|  | IA-5(1) | L,M,H |  |  |  |  |
|  | IA-5(2) | M,H |  |  |  |  |
|  | IA-5(3) | M,H |  |  |  |  |
| IA-6 |  | L,M,H | Authenticator Feedback |  |  |  |
| IA-7 |  | L,M,H | Cryptographic Module Authentication |  |  |  |
| IA-8 |  | L,M,H | Identification and Authentication (Non-Organizational Users) |  |  |  |
| Incident Response | | | |  |  |  |
| IR-1 |  | L,M,H | Incident Response Policy and Procedures |  |  |  |
| IR-2 |  | L,M,H | Incident Response Training |  |  |  |
|  | IR-2(1) | H |  |  |  |  |
|  | IR-2(2) | H |  |  |  |  |
| IR-3 |  | L,M,H | Incident Response Testing |  |  |  |
|  | IR-3(1) | H |  |  |  |  |
| IR-4 |  | M,H | Incident Handling |  |  |  |
|  | IR-4(1) | M,H |  |  |  |  |
| IR-5 |  | L,M,H | Incident Monitoring |  |  |  |
|  | IR-5(1) | H |  |  |  |  |
| IR-6 |  | L,M,H | Incident Reporting |  |  |  |
|  | IR-6(1) | M,H |  |  |  |  |
| IR-7 |  | L,M,H | Incident Response Assistance |  |  |  |
|  | IR-7(1) | M,H |  |  |  |  |
| IR-8 |  | L,M,H | Incident Response Plan |  |  |  |
| Maintenance | | | |  |  |  |
| MA-1 |  | L,M,H | System Maintenance Policy and Procedures |  |  |  |
| MA-2 |  | L,M,H | Controlled Maintenance |  |  |  |
|  | MA-2(1) | M,H |  |  |  |  |
|  | MA-2(2) | H |  |  |  |  |
| MA-3 |  | M,H | Maintenance Tools |  |  |  |
|  | MA-3(1) | M,H |  |  |  |  |
|  | MA-3(2) | M,H |  |  |  |  |
|  | MA-3(3) | H |  |  |  |  |
| MA-4 |  | L,M,H | Remote Maintenance |  |  |  |
|  | MA-4(1) | M,H |  |  |  |  |
|  | MA-4(2) | M,H |  |  |  |  |
|  | MA-4(3) | H |  |  |  |  |
| MA-5 |  | L,M,H | Maintenance Personnel |  |  |  |
| MA-6 |  | M,H | Timely Maintenance |  |  |  |
| Media Protection | | | |  |  |  |
| MP-1 |  | L,M,H | Media Protection Policy and Procedures |  |  |  |
| MP-2 |  | L,M,H | Media Access |  |  |  |
|  | MP-2(1) | M,H |  |  |  |  |
| MP-3 |  | M,H | Media Labeling |  |  |  |
| MP-4 |  | M,H | Media Storage |  |  |  |
| MP-5 |  | M,H | Media Transport |  |  |  |
|  | MP-5(2) | M,H |  |  |  |  |
|  | MP-5(3) | H |  |  |  |  |
|  | MP-5(4) | M,H |  |  |  |  |
| MP-6 |  | L,M,H | Media Sanitization and Destruction/Disposal |  |  |  |
|  | MP-6(1) | H |  |  |  |  |
|  | MP-6(2) | H |  |  |  |  |
| Physical and Environmental Protection | | | |  |  |  |
| PE-1 |  | L,M,H | Physical and Environmental Protection Policy and Procedures |  |  |  |
| PE-2 |  | L,M,H | Physical Access Authorizations |  |  |  |
| PE-3 |  | L,M,H | Physical Access Control |  |  |  |
|  | PE-3(1) | H |  |  |  |  |
| PE-4 |  | H | Access Control for Transmission Medium |  |  |  |
| PE-5 |  | M,H | Access Control for Output Devices |  |  |  |
| PE-6 |  | L,M,H | Monitoring Physical Access |  |  |  |
|  | PE-6(1) | M,H |  |  |  |  |
|  | PE-6(2) | H |  |  |  |  |
| PE-7 |  | L,M,H | Visitor Control |  |  |  |
|  | PE-7(1) | M,H |  |  |  |  |
| PE-8 |  | L,M,H | Access Logs |  |  |  |
|  | PE-8(1) | H |  |  |  |  |
|  | PE-8(2) | H |  |  |  |  |
| PE-9 |  | M,H | Power Equipment and Power Cabling |  |  |  |
| PE-10 |  | M,H | Emergency Shutoff |  |  |  |
| PE-11 |  | M,H | Emergency Power |  |  |  |
|  | PE-11(1) | H |  |  |  |  |
| PE-12 |  | L,M,H | Emergency Lighting |  |  |  |
| PE-13 |  | L,M,H | Fire Protection |  |  |  |
|  | PE-13(1) | M,H |  |  |  |  |
|  | PE-13(2) | M,H |  |  |  |  |
|  | PE-13(3) | M,H |  |  |  |  |
| PE-14 |  | L,M,H | Temperature and Humidity Controls |  |  |  |
| PE-15 |  | L,M,H | Water Damage Protection |  |  |  |
|  | PE-15(1) | H |  |  |  |  |
| PE-16 |  | L,M,H | Delivery and Removal |  |  |  |
| PE-17 |  | M,H | Alternate Work Site |  |  |  |
| PE-18 |  | M,H | Location of Information System Components |  |  |  |
|  | PE-18(1) | H |  |  |  |  |
| PE-19 |  | NS | Information Leakage |  |  | N/A - Not Selected |
| Planning | | | |  |  |  |
| PL-1 |  | L,M,H | Security Planning Policy and Procedures |  |  |  |
| PL-2 |  | L,M,H | System Security Plan |  |  |  |
| PL-3 |  |  | System Security Plan Update |  |  | Withdrawn from rev.3 |
| PL-4 |  | L,M,H | Rules of Behavior |  |  |  |
| PL-5 |  | L,M,H | Privacy Impact Assessment |  |  |  |
| PL-6 |  | L,M,H | Security-Related Activity Planning |  |  |  |
| Personnel Security | | | |  |  |  |
| PS-1 |  | L,M,H | Personnel Security Policy and Procedures |  |  |  |
| PS-2 |  | L,M,H | Position Categorization |  |  |  |
| PS-3 |  | L,M,H | Personnel Screening |  |  |  |
| PS-4 |  | L,M,H | Personnel Termination |  |  |  |
| PS-5 |  | L,M,H | Personnel Transfer |  |  |  |
| PS-6 |  | L,M,H | Access Agreements |  |  |  |
| PS-7 |  | L,M,H | Third-Party Personnel Security |  |  |  |
| PS-8 |  | L,M,H | Personnel Sanctions |  |  |  |
| Risk Assessment | | | |  |  |  |
| RA-1 |  | L,M,H | Risk Assessment Policy and Procedures |  |  |  |
| RA-2 |  | L,M,H | Security Categorization |  |  |  |
| RA-3 |  | L,M,H | Risk Assessment |  |  |  |
| RA-4 |  |  | Risk Assessment Update |  |  | Withdrawn from rev 3 |
| RA-5 |  | L,M,H | Vulnerability Scanning |  |  |  |
|  | RA-5(1) | M,H |  |  |  |  |
|  | RA-5(2) | H |  |  |  |  |
|  | RA-5(3) | H |  |  |  |  |
|  | RA-5(4) | H |  |  |  |  |
|  | RA-5(5) | H |  |  |  |  |
|  | RA-5(7) | H |  |  |  |  |
| System and Services Acquisition | | | |  |  |  |
| SA-1 |  | L,M,H | System and Services Acquisition Policy and Procedures |  |  |  |
| SA-2 |  | L,M,H | Allocation of Resources |  |  |  |
| SA-3 |  | L,M,H | Life Cycle Support |  |  |  |
| SA-4 |  | L,M,H | Acquisitions |  |  |  |
|  | SA-4(1) | M,H |  |  |  |  |
|  | SA-4(2) | H |  |  |  |  |
|  | SA-4(4) | M,H |  |  |  |  |
| SA-5 |  | L,M,H | Information System Documentation |  |  |  |
|  | SA-5(1) | M,H |  |  |  |  |
|  | SA-5(2) | H |  |  |  |  |
| SA-6 |  | L,M,H | Software Usage Restrictions |  |  |  |
| SA-7 |  | L,M,H | User Installed Software |  |  |  |
| SA-8 |  | M,H | Security Engineering Principles |  |  |  |
| SA-9 |  | L,M,H | External Information System Services |  |  |  |
| SA-10 |  | M,H | Developer Configuration Management |  |  |  |
| SA-11 |  | M,H | Developer Security Testing |  |  |  |
| SA-12 |  | H | Supply Chain Protection |  |  |  |
| SA-13 |  | H | Trustworthiness |  |  |  |
| SA-14 |  | NS | Critical Information System Components |  |  | N/A - Not Selected |
| System and Communications Protection | | | |  |  |  |
| SC-1 |  | L,M,H | System and Communications Protection Policy and Procedures |  |  |  |
| SC-2 |  | M,H | Application Partitioning |  |  |  |
| SC-3 |  | H | Security Function Isolation |  |  |  |
| SC-4 |  | M,H | Information Shared Resources |  |  |  |
| SC-5 |  | L,M,H | Denial of Service Protection |  |  |  |
| SC-6 |  | NS | Resource Priority |  |  | N/A - Not Selected |
| SC-7 |  | L,M,H | Boundary Protection |  |  |  |
|  | SC-7(1) | M,H |  |  |  |  |
|  | SC-7(2) | M,H |  |  |  |  |
|  | SC-7(3) | M,H |  |  |  |  |
|  | SC-7(4) | M,H |  |  |  |  |
|  | SC-7(5) | M,H |  |  |  |  |
|  | SC-7(6) | H |  |  |  |  |
|  | SC-7(7) | M,H |  |  |  |  |
|  | SC-7(8) | H |  |  |  |  |
| SC-8 |  | M,H | Transmission Integrity |  |  |  |
|  | SC-8(1) | M,H |  |  |  |  |
| SC-9 |  | M,H | Transmission Confidentiality |  |  |  |
|  | SC-9(1) | M,H |  |  |  |  |
| SC-10 |  | M,H | Network Disconnect |  |  |  |
| SC-11 |  | NS | Trusted Path |  |  | N/A - Not Selected |
| SC-12 |  | L,M,H | Cryptographic Key Establishment and Management |  |  |  |
|  | AC-12(1) | H |  |  |  |  |
| SC-13 |  | L,M,H | Use of Validated Cryptography |  |  |  |
| SC-14 |  | L,M,H | Public Access Protections |  |  |  |
| SC-15 |  | L,M,H | Collaborative Computing |  |  |  |
| SC-16 |  | NS | Transmission of Security Attributes |  |  | N/A - Not Selected |
| SC-17 |  | M,H | Public Key Infrastructure Certificates |  |  |  |
| SC-18 |  | M,H | Mobile Code |  |  |  |
| SC-19 |  | M,H | Voice Over Internet Protocol |  |  |  |
| SC-20 |  | L,M,H | Secure Name /Address Resolution Service (Authoritative Source) |  |  |  |
|  | SC-20(1) | L,M,H |  |  |  |  |
| SC-21 |  | H | Secure Name /Address Resolution Service (Recursive or Caching Resolver) |  |  |  |
| SC-22 |  | M,H | Architecture and Provisioning for Name/Address Resolution Service |  |  |  |
| SC-23 |  | M,H | Session Authenticity |  |  |  |
| SC-24 |  | H | Fail in Known State |  |  |  |
| SC-25 |  | NS | Thin Nodes |  |  | N/A - Not Selected |
| SC-26 |  | NS | Honey pots |  |  | N/A - Not Selected |
| SC-27 |  | NS | Operating System-Independent Applications |  |  | N/A - Not Selected |
| SC-28 |  | M,H | Protection of Information at Rest |  |  |  |
| SC-29 |  | NS | Heterogeneity |  |  | N/A - Not Selected |
| SC-30 |  | NS | Virtualization Techniques |  |  | N/A - Not Selected |
| SC-31 |  | NS | Covert Channel Analysis |  |  | N/A - Not Selected |
| SC-32 |  | M,H | Information System Partitioning |  |  |  |
| SC-33 |  | NS | Transmission Preparation Integrity |  |  | N/A - Not Selected |
| SC-34 |  | NS | Non-Modifiable Executable Programs |  |  | N/A - Not Selected |
| System and Information Integrity | | | |  |  |  |
| SI-1 |  | L,M,H | System and Information Integrity Policy and Procedures |  |  |  |
| SI-2 |  | L,M,H | Flaw Remediation |  |  |  |
|  | SI-2(1) | H |  |  |  |  |
|  | SI-2(2) | M,H |  |  |  |  |
| SI-3 |  | L,M,H | Malicious Code Protection |  |  |  |
|  | SI-3(1) | M,H |  |  |  |  |
|  | SI-3(2) | M,H |  |  |  |  |
|  | SI-3(3) | M,H |  |  |  |  |
| SI-4 |  | M,H | Intrusion Detection Tools and Techniques |  |  |  |
|  | SI-4(2) | M,H |  |  |  |  |
|  | SI-4(4) | M,H |  |  |  |  |
|  | SI-4(5) | M,H |  |  |  |  |
|  | SI-4(6) | M,H |  |  |  |  |
| SI-5 |  | L,M,H | Security Alerts and Advisories |  |  |  |
|  | SI-5(1) | H |  |  |  |  |
| SI-6 |  | H | Security Functionality Verification |  |  |  |
| SI-7 |  | H | Software and Information Integrity |  |  |  |
|  | SI-7(1) | H |  |  |  |  |
|  | SI-7(2) | H |  |  |  |  |
| SI-8 |  | M,H | Spam and Spyware Protection |  |  |  |
|  | SI-8(1) | H |  |  |  |  |
| SI-9 |  | M,H | Information Input Restrictions |  |  |  |
| SI-10 |  | M,H | Information Input Accuracy, Completeness, and Validity |  |  |  |
| SI-11 |  | M,H | Error Handling |  |  |  |
| SI-12 |  | M,H | Information Output Handling and Retention |  |  |  |
| SI-13 |  | NS | Predictable Failure Prevention |  |  | N/A - Not Selected |
| 0 | 155 |  | Totals |  |  | 20 |