Global Information Assurance Certification Paper

Mike Frandsen

October 17, 2003

SANS GIAC Security Leadership Certificate (GSLC) Assignment, Version 1.0

Network Interconnection Security Agreement (ISA)

Organization A NETWORK INTERCONNECTION SECURITY AGREEMENT (NETWORK ISA)

ABSTRACT/SELECTION CRITERIA/APPLICABILITY

This Network Interconnection Security Agreement (ISA) is intended to minimize security risks and ensure the confidentiality, integrity, and availability of the sensitive but unclassified information of a federal agency (Organization A) as well as the information that is owned by an external organization (Organization B) that has a network interconnection[1] with Organization A. Examples of network interconnections may include dedicated T-1 lines or corporate Virtual Private Network (VPN) tunnels that are used to connect to a network. This Network ISA ensures the adequate security of Organization A information being accessed over the Organization A Network and provides that all network access satisfy the mission requirements of both Organization A and Organization B.

Organization A has established network interconnections with business partners to advance the mission of Organization A. Business partners include other government agencies and commercial organizations. These interconnections increase efficiency and functionality, reduce costs, and improve management of information. If not properly managed, however, information technology (IT) system and network interconnections can result in unacceptable security risks that can potentially compromise all connected IT systems and the data they store, process, or transmit, as well as networks connected to those systems. The Network ISA is designed to prevent security incidents such as viruses or hacker attacks from spreading from one network to another. One compromised system on one network can easily spread to other parts of the network and any networks that are interconnected.

This Network ISA will help minimize the costly loss of person-hours to remediate security incidents that would be more likely to result without agreed upon policies, procedures, and implementations of IT security best practices. This Network ISA will allow federal government agencies to ensure that IT security controls facilitate the mission of their agencies without causing disruptions to the mission. Network interconnections have proliferated with the growth of the Internet; however, documentation and security controls have not kept pace with the growth of networks. By examining all network interconnections, organizations may determine that connections are no longer required, or may be reengineered to meet security requirements and support organization missions.

Federal policy requires agencies to develop interconnection agreements for federal systems/networks that share or exchange information with external systems/networks. This Network ISA is based largely[2] on the format in the National Institute of Standards and Technology *Security Guide for Interconnecting Information Technology Systems*

---

[1] A***"network interconnection"*** is defined as the direct connection of two or more IT networks for the purpose of sharing data and other information resources. (This is based on the definition of system interconnection in NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems)

[2] Note: The templates in NIST SP 800-47 are the basis for this document. For sections in which a majority of the wording was taken from NIST SP 800-47, the text is in italics, and this source is listed in parentheses as follows: (NIST SP 800-47). Wording in italics without the source cited is also from NIST SP 800-47.

(NIST Special Publication 800-47 - http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf). The templates in NIST SP 800-47 have been modified and added to so that a federal government agency can use this template for situations in which networks interconnect. Organizations may use this template to develop ISAs of their own. Organizations may wish to modify some of the text to be consistent with their missions and security requirements. NIST SP 800-47 states: "A system that is approved by an Interconnection System Agreement (ISA) for interconnection with one organization's system shall meet the protection requirements equal to, or greater than, those implemented by the other organization's system." The guidelines establish security measures that shall be taken to protect the connected systems/networks and shared data. Organization A IT managers and security personnel shall comply with the NIST guidelines in managing the process of interconnecting systems/networks.

This Network ISA documents interconnection arrangements and security responsibilities for Organization A and Organization B, outlines security safeguards, and provides the technical and operational security requirements. This Network ISA also specifies business and legal requirements for the networks being interconnected. This Network ISA authorizes mutual permission to connect Organization A's Network and Organization B's Network and establishes a commitment to protect data that is exchanged between the networks or processed and stored on systems that reside on the networks. Through this Network ISA, Organization A and Organization B shall minimize the susceptibility of their connected systems/networks to IT security risks and aid in mitigation and recovery from IT security incidents.

Organization A NETWORK INTERCONNECTION SECURITY AGREEMENT (NETWORK ISA)

TABLE OF CONTENTS

1 PURPOSE…….. 6

2 BACKGROUND…… 6

2.1 ORGANIZATION A…… 6
2.2 Organization A IT Security Program…… 6
2.3 Organization A Computer Emergency Response Capability …….. 6
2.4 Information Security Officers…… 7
2.5 Organization B……7

3 SCOPE…… 7

4 AUTHORITY…… 7

5 STATEMENT OF REQUIREMENTS…….. 8

5.1 General Information/Data Description…… 8
5.2 Services Offered…….. 8

6 NETWORK DESCRIPTIONS…….. 8

6.1 Organization A Network …….. 8
6.2 Network B Network…… 9
6.3 Topological Diagram…… 9

7 SECURITY RESPONSIBILITIES…… 9

7.1 Communication/IT Security Points of Contact…….. 9
7.2 Responsible Parties…….. 10

8 PERSONNEL/USER SECURITY……..11

8.1 User Community…… 11
8.2 Commitment to Protect Sensitive Information……11
8.3 Authorized Use…… 12
8.4 Training and Awareness…….. 12
8.5 Personnel Changes/Deregistration…… 12

9 POLICIES…… 13

9.1 Security Rules of Conduct…… 13
9.2 Trusted Behavior Expectations…….. 14
9.3 Security Documentation
9.4 Information Exchange Security…….. 14
9.5 Specific Equipment Restrictions/Physical Security…… 14

10 NETWORK SECURITY…… 15

10.1 Network Management…… 15
10.2 Material Network Changes……15
10.3 New Interconnections…… 16
10.4 Network Inventory…… 16

10.5 Firewall Management…….. 16

11 INCIDENT PREVENTION, DETECTION, AND RESPONSE…….. 16

11.1 Incident Handling……16
11.2 Vulnerability Scanning…….. 18
11.3 Disasters and Other Contingencies…….. 19

12 HOST SECURITY……19

12.1 Identification and Authentication……19
12.2 Anti-Virus Software……19
12.3 System Configuration…….. 19
12.4 Backups…….. 19
12.5 Disposal of IT Equipment…… 20
12.6 Warning Banners…….. 20

13 EXTERNAL ACCESS…… 20

13.1 Remote Access……20
13.2 Wireless Security…….. 20

14 COMPLIANCE……20

15 SIGNATURES…… 21

1 PURPOSE

The purpose of this Network ISA is to establish procedures of reciprocal cooperation and coordination between Organization A, a federal government agency, and Organization B, a business partner, regarding the development, management, operation, and security of a connection between the Organization A Network, owned by Organization A, and the Organization B Network, owned by Organization B (NIST SP 800-47).

2 BACKGROUND

2.1 Organization A

[*Describe the background and mission of the organization.***]**

2.2 Organization A IT Security Program

The Organization A IT Security Program helps Organization A accomplish its mission by ensuring the confidentiality, integrity, and availability of Organization A information resources. The Organization A IT Security Program has developed policies and guidelines that ensure the adequate security of agency information and comply with Federal laws and regulations. Organization A monitors the security of the Organization A Network 24 hours a day, seven days a week (24 x 7), through management, operational, and technical processes. Training initiatives are continuously updated to ensure that managers, users, and technical personnel are aware that they are responsible for the adequate security of their systems.

2.3 Organization A Computer Emergency Response Capability

The Organization A Computer Emergency Response Capability (CERC) ensures the IT security of the multi-platform computing environment necessary to conduct and manage the Organization A mission by serving as the focal point for IT security incidents. The Organization A CERC monitors the security of the Organization A Network 24 x 7 through the expertise of IT security professionals and automated IT security processes. Organization A CERC members are trained in identifying and investigating IT security incidents such as web defacements, computer compromises, and viruses. The Organization A CERC is continuously enhancing its IT security auditing methods and incident handling procedures.

2.4 Information Security Officers

The Organization A Senior Information Security Officer (SISO) supports and implements the Organization A IT security program. The Organization A SISO directs, coordinates, and evaluates the security policy of Organization A. An Information Security Officer (ISO) represents each division of Organization A and implements standardized

information security policies across Organization A concerning the confidentiality, availability, and integrity of information resources. Although the ISOs directly report to the management of their division, as part of their security responsibilities the ISOs have responsibilities to the Organization A SISO and thus to the Organization A CIO. In the IT security role ISOs take direction from the Organization A CIO or the Organization A SISO when action is required to protect Organization A assets from attack. The Organization A SISO and ISOs will work with Organization B to enhance IT security measures. See Section 7.1, *Communication/IT Security Points of Contact*, for additional information on the role of ISOs.

2.5 Organization B

[*Insert background information about Organization B, including a brief description of the organization, its mission, and its IT security program***]**.

3 SCOPE

- This Network ISA applies to the network interconnection between the Organization A Network and the network subnet or subnets of Organization B's Network that are required to connect to the Organization A Network for Organization A and Organization B mission related needs.
- This Network ISA applies to all IT systems that reside on Organization B's Network and its interconnection with the Organization A Network, whether they are owned by Organization A, other government agencies, or non-government organizations.
- This Network ISA applies to all Organization B personnel and any other persons using IT equipment or accessing Organization A systems. This includes Organization A and Organization B employees, contractors and subcontractors; and other federally and non-federally funded users managing, engineering, accessing, or utilizing Organization B's Network.
- This Network ISA applies to all related network components such as hosts, routers, and switches; IT devices that assist in managing security such as firewalls, intrusion detection systems (IDS), and vulnerability scanning tools; desktop workstations; servers; and major applications.
- All existing and future users of and equipment deployed on Organization B's Network shall comply with this Network ISA.
- Organization A and Organization B subnets that are not part of this network interconnection are not within the scope of this Network ISA.
- By interconnecting with the Organization A Network, Organization B agrees to be bound by this Network ISA and use the Organization A Network in compliance with this Network ISA.

4 AUTHORITY

The authority for this Network ISA is based on the following laws, policies, and regulations:

- Computer Security Act of 1987 (P.L. 100-235)
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems*
- Federal Information Security Management Act (FISMA) of 2002 [Title X of the Homeland Security Act of 2002 (P.L. 107-296) and Title III of the E-Government Act of 2002 (P.L. 107-347)]

This Network ISA is also in compliance with all Organization A policies.

5 STATEMENT OF REQUIREMENTS

This Network ISA governs the relationship between Organization A and Organization B regarding Organization B's connection to and use of the Organization A Network.

It is the intent of both parties of this Network ISA to interconnect the IT systems/networks listed below to exchange data between Organization A and Organization B. Organization B requires the use of the Organization A Network, as approved and directed by the Organization A Chief Information Officer ("Organization A CIO"). Organization A may require the use of Organization B's network (NIST SP 800-47). ***[****Describe the expected benefit of the interconnection.****]***

5.1 General Information/Data Description

[*Describe the information and data that will be made available, exchanged, or passed one-way only by the interconnection of the two systems/networks.***]**

6 NETWORK DESCRIPTIONS

6.1 Organization A Network

The Organization A Network is the Organization A backbone network. It interconnects the Organization A local area networks (LANs) with the Internet and other government agencies.

6.1.1 Name: Organization A Network

6.1.2 Function:

6.1.3 Location: [*Include address or termination point of network interconnection including building number, floor and room number***].**

6.1.4 Description of Data, including Sensitivity or Classification Levels:

Category of Safeguarded Agency Information: Sensitive

Security Level Designations for Agency Information:

- **Level of Sensitivity of Data**
- **Level of Operational Criticality of the Data Processing Capabilities**
- **Overall Security Level Designation**

6.2 Network B

6.2.1 Name: Organization B Network

6.2.2 Function:

6.2.3 Location: [*Include address or termination point of network interconnection including building number, floor and room number***].**

6.2.4 Description of data, including Sensitivity or Classification level:

Category of Safeguarded Agency Information: Sensitive

- **Level of Sensitivity of Data**
- **Level of Operational Criticality of the Data Processing Capabilities**
- **Overall Security Level Designation**

6.3 Topological Diagram [*Insert here or add as attachment.*]

7 SECURITY RESPONSIBILITIES

Mutual Responsibilities

Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained in The Organization A Network and Organization B's Network, whichever is greater.

7.1 Communication/IT Security Points of Contact

Mutual Responsibilities

Frequent formal communications are essential to ensure the successful management and operation of the interconnection. The parties to this Network ISA agree to maintain open lines of communication between designated staff at both the managerial and technical levels (NIST SP 800-47).

Organization A NETWORK INTERCONNECTION SECURITY AGREEMENT (NETWORK ISA)

The owners of The Organization A Network and Organization B Network agree to designate and provide contact information for technical leads for their respective network, and to facilitate direct contacts between technical leads to support the management and operation of the interconnection. In the event that the technical leads of either organization change, each organization shall be promptly informed (NIST SP 800-47).

Organization A Responsibilities

- Provide an ISO to serve as a liaison between Organization A and Organization B, assist Organization B in implementing and managing its IT security program, and assist Organization B in ensuring that its IT security controls meet or exceed Organization A requirements. The ISO shall contact the Organization A CERC on behalf of Organization B for issues involving security incidents.
- Add the Organization B POC to the ISO Listserv.

Organization B Responsibilities

Designate an IT security Point of Contact (POC), who shall act on behalf of Organization B and communicate all IT security issues involving Organization B to Organization A via the ISO. The Organization B POC shall be the Organization B ISO or another IT security official who shall be responsible for implementing and managing Organization B's IT security program and ensuring that Organization B IT security controls meet or exceed Organization A requirements.

7.2 Responsible Parties

A. Organization A SISO:
Address:

Work Phone:
Cell Phone:
Fax:
E-Mail:
Supervisor:

B. Organization A ISO
Title:
Address:

Work Phone:
Cell Phone:
Fax:
E-Mail:
Supervisor:

C. Organization B POC:
Title:
Address:

Work Phone:
Cell Phone:
Fax:
E-Mail:
Supervisor:

8 PERSONNEL/USER SECURITY

8.1 User Community

Mutual Responsibilities

Ensure that all employees, contractors, and other authorized users with access to the Organization A Network and Organization B and the data sent and received from either organization are not security risks.

8.2 Commitment to Protect Sensitive Information

Mutual Responsibilities

Do not release, publish, or disclose information to unauthorized personnel, and protect such information in accordance with provisions of the following laws and any other pertinent laws and regulations governing the adequate safeguard of agency information (NIST SP 800-47):

- 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records)
- 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)
- Paperwork Reduction Act of 1995 (44 U.S.C. ch. 35)
- Privacy Act of 1974 (5 U.S.C. § 552a)

Ensure that all information from each organization has a level of security that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information.

Organization B Responsibilities

- Ensure that each Organization B contractor employee signs an appropriate Non-Disclosure Agreement.
- Ensure that outsourced operations where non-Organization A personnel may have access to information, critical Organization A systems, and network components

shall also comply with the security required by Federal Acquisition Regulation (FAR) clause 52.239-1, *Privacy or Security Safeguards*.

8.3 Authorized Use

Mutual Responsibilities

- Ensure that users adhere to the Organization A Policy on Acceptable Personal Use. *Limited personal* use is allowed under the restrictions of this policy; however, any non-Organization A commercial business conducted on Organization A resources is prohibited.
- Inform users that they shall not transmit sensitive Organization A information to any personal or non-Organization A related business e-mail account.

8.4 Training and Awareness

Mutual Responsibilities

All users, including employees, contractors, and other authorized users with access to the Organization A Network shall complete a federally-approved IT security awareness course annually or an equivalent annual training and awareness course. The level of training shall be commensurate with the individual's duties and responsibilities.

Organization B Responsibilities

Ensure that Organization B users, including employees, contractors, and other authorized users are familiar with Organization A training and awareness requirements.

8.5 Personnel Changes/Deregistration

Mutual Responsibilities (NIST SP 800-47)

- *Provide notification of the separation or long-term absence of the respective network owner or technical lead.*
- *Provide notification of any changes in ISO or POC information.*
- *Provide notification of changes to user profiles, including users who resign or change job responsibilities.*
- Ensure that user accounts are deregistered when staff no longer need them.

Organization B Responsibilities

Inform the ISO of all deregistration actions and all actions taken to create new accounts.

9 POLICIES

Mutual Responsibilities

- *Each network shall protect information belonging to the other through the implementation of security controls that adequately safeguard against intrusion, tampering, viruses and other security breaches (NIST SP 800-47).*
- Adhere to all Organization A IT security policies, procedures, and guidelines and NIST special publications at http://csrc.nist.gov/publications/nistpubs/.
- Enforce the following IT security best practices:
  - Least Privilege: Only authorize access to the minimum amount of resources required for a function.
  - Separation of Duties: Functions shall be divided between staff members to reduce the threat that one person can commit fraud undetected.
  - Role-Based Security: Access control shall be based on the role a user plays in an organization.

Organization B Responsibilities

Adhere to IT security policies, guidelines, and procedures at least as stringent as those listed on the Organization A IT security web site. Apply stricter policies where appropriate.

9.1 Security Rules of Conduct

Mutual Responsibilities

All users with access to the Organization A Network and the Organization B Network and any data received from the other organization shall adhere to all current Organization A Security Rules of Conduct.

9.2 Trusted Behavior Expectations

Mutual Responsibilities

Protect the information on each network in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a); the Trade Secrets Act (18 U.S.C. § 1905; and Title II of the Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2701-2712). (NIST SP 800-47).

9.3 Security Documentation

Mutual Responsibilities

Organization A NETWORK INTERCONNECTION SECURITY AGREEMENT (NETWORK ISA)

For each IT system, security shall be planned for, documented, and integrated into the System Life Cycle from the IT system's initiation to the system's disposal. (NIST SP 800-47).

Organization A Responsibilities

- Provide Organization B with access to all Organization A IT security policies, procedures, and guidelines.
- Update the Organization A Network Security Plan every three years or when a major modification has been made to the network.

Organization B Responsibilities

- Provide documentation to Organization A that Organization B has an IT security program that meets or exceeds federal requirements, including any security policies, whitepapers, or other technical documents.
- Ensure that the general support system/LAN on which Organization B resources reside meets or exceeds the requirements of the Organization A Network Security Plan that describes all in-place security controls protecting the system and delineates responsibilities and expected behavior of all individuals who access the system.
- If a major modification is made to the general support system/LAN on which Organization B resources reside, develop a Security Plan and submit it to the ISO. The Security Plan shall be based on NIST SP 800-18: *Guide for Developing Security Plans for IT Systems* at http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF.

9.4 Information Exchange Security

Mutual Responsibilities

- Ensure that data being stored or transmitted is protected commensurate with its sensitivity and criticality levels and the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information.

- Use NIST-approved encryption to protect highly sensitive (Level 3) Organization A data in storage and in transit over a public network such as the Internet. Federal Information Processing Standards (FIPS) approved encryption algorithms and links to their standards are available at http://csrc.nist.gov/CryptoToolkit/tkencryption.html. Approved algorithms include the Data Encryption Standard (DES - for legacy applications only), Triple DES, the Advanced Encryption System (AES).

9.5 Specific Equipment Restrictions/Physical Security

Mutual Responsibilities

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 (NIST SP 800-47).

10 NETWORK SECURITY

10.1 Network Management

Organization B Responsibilities

- Restrict contractor employees and other non-governmental personnel from using resources on Organization B's Network unless they are supporting the purpose of the interconnection between the Organization A Network and Organization B's Network.
- Ensure that there are no direct Internet connections from Organization B's Network. Internet access shall be provided only through the main Organization A Network Internet access gateway.
- Ensure that Organization B's Network is completely isolated from any other network or customer/business partner that Organization B has in place so there is no direct access between the networks, and the networks use separate hosts and separate infrastructure.

10.2 Material Network Changes

Mutual Responsibilities

Proposed changes to either network that affect the interconnecting medium or to the interconnecting medium itself shall be accompanied by a valid business justification submitted to the Organization A CIO, and are subject to security review to determine the potential impact on the interconnection. This Network ISA shall be renegotiated before any changes are implemented.

Planned technical changes to the network architecture that affect the interconnection shall be reported through the ISO to the Organization A CERC and Organization B before such changes are implemented. The initiating party agrees to initiate a risk assessment based on the new network architecture and to modify and re-sign this Network ISA within one (1) month prior to implementation (NIST SP 800-47).

Organization B Responsibilities

Notify the ISO when access is no longer required. The ISO shall inform the Organization A CERC, which shall then terminate the access.

10.3 New Interconnections

Mutual Responsibilities

New interconnections between Organization A and Organization B are prohibited unless expressly agreed upon in a modification to this Network ISA signed by both parties.

10.4 Network Inventory

Organization B Responsibilities

Maintain a list of all Organization B subnets connected to the Organization A Network and periodically update the information. Include information on each system's owner, physical location, IP address, hostname, hardware, operating system version, and major applications. Make the inventory available to Organization A when requested.

10.5 Firewall Management

Organization A Responsibilities

- Configure the Organization A perimeter firewall in accordance with the Organization A Firewall Policy. Block all network traffic incoming from the Internet to the Organization A Network unless it is explicitly permitted.
- Install a firewall between the perimeter (demarcation point) of Organization B's Network and the Organization A Network if deemed necessary by the Organization A CERC.

Organization B Responsibilities

- Maintain responsibility for configuring all Organization B network perimeter firewalls with a policy at least as stringent as the Organization A Firewall Policy.
- Send any proposed firewall policy changes to the ISO who shall send them to the Organization A CERC.
- Inform the ISO of any use of Network Address Translation (NAT).

11 INCIDENT PREVENTION, DETECTION, AND RESPONSE

11.1 Incident Handling

Mutual Responsibilities

Organization A NETWORK INTERCONNECTION SECURITY AGREEMENT (NETWORK ISA)

This Network ISA between Organization A and Organization B establishes a mechanism for Organization B to utilize the existing expertise of the Organization A CERC through the ISO to ensure the confidentiality, integrity, and availability of Organization A and Organization B information resources that are connected to the Organization A Network.

Technical staff shall immediately notify their designated counterparts by telephone or e-mail when a security incident is detected, so the other party may take steps to determine whether its network has been compromised and take appropriate security precautions. The ISO and Organization B POC shall receive formal e-mail notification within 24 hours of detection of the incident(s) from the Organization A CERC (NIST SP 800-47).

Organization A Responsibilities

- Disseminate intrusion detection alerts to the ISO of the division whose subnets are connected to Organization B's Network and the Organization B POC.
- Report any security incident discovered by Organization A that affects Organization B's subnets to the ISO and the Organization B POC.
- Block inbound and outbound access for any Organization A or Organization B systems on the subnets connected to the Organization A Network that are the source of incidents.
- In the event of multiple incidents that occur on Organization B's Network that are major in scope and threaten the security of the Organization A Network, Organization A shall block inbound and outbound access between the Organization A Network and Organization B's Network after informing the Organization B CIO. Service shall be restored once incidents have been sufficiently remediated to minimize risk.
- Provide 24 x 7 service to the ISO representing Organization B in case of IT security emergencies.
- Periodically update the Organization A CERC IT Security Bulletins web site with advice on preventing, detecting, and responding to incidents, and send advisories to the ISO representing Organization B. The ISO is responsible for forwarding this information to the Organization B POC.

Organization B Responsibilities

- The Organization B POC shall report any security incidents discovered by Organization B to the ISO, who shall report them to the Organization A CERC.
- Conduct remediation of any successful incidents (compromises) and report status to the ISO who will inform the Organization A CERC or request that the Organization A CERC provide assistance when necessary.

- Provide 24 x 7 contact information that Organization A can use to communicate with Organization B in case of IT security emergencies.
- Periodically check the Organization A CERC IT Security Bulletins web site for advice on preventing, detecting, and responding to incidents.

11.2 Vulnerability Scanning

Mutual Responsibilities

Conduct vulnerability scans to identify any potential security vulnerabilities based on the SANS Twenty Most Critical Internet Security Vulnerabilities at http://isc.sans.org/top20.html.

Organization A Responsibilities

- Communicate with the ISO, who shall notify the Organization B POC to ensure that all responsible parties are aware of the time and scope of each scan.
- Provide confidential reports to Organization B categorizing and prioritizing all vulnerabilities and recommending corrective actions.

Organization B Responsibilities

- Notify the ISO of any scans that Organization B decides to conduct that may be misinterpreted as malicious activity.
- Review vulnerability reports, ensure remediation is conducted, and notify the ISO of the status of remediation.

11.3 Disasters and Other Contingencies

Mutual Responsibilities

Technical staff shall 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 networks (NIST SP 800-47). The Organization A CERC and the Organization B POC shall communicate to each other through the ISO. In response to a disaster, one or both organizations may decide to terminate the interconnection for security reasons.

12 HOST SECURITY

12.1 Identification and Authentication

Mutual Responsibilities

- *Individual users shall not have access to the data except through their systems security software inherent to the operating system. All access shall be controlled by authentication methods to validate the approved users (NIST SP 800-47).* Access to systems shall be conducted in compliance with the Organization A Password Guidance which states that passwords must not be shared, must be changed monthly, and must contain at least 8 mixed alphabetic, numeric, and special characters.
- Ensure the implementation and enforcement of user identification and authentication techniques for IT systems and networks according to NIST-approved standards for implementing user and message authentication mechanisms.

12.2 Anti-Virus Software

Organization A Responsibilities

Ensure that government-approved anti-virus software is installed, updated, and configured to periodically scan at the perimeter between the Organization A Network and the Internet, on Organization A e-mail servers, and Organization A desktop workstations.

Organization B Responsibilities

Ensure that anti-virus software is installed, updated, and configured to periodically scan at the perimeter (demarcation point) between Organization B's Network and the Organization A Network, and on any servers and desktop workstations (computers) that reside on Organization B's Network. Virus scans shall occur at least daily.

12.3 System Configuration

Mutual Responsibilities

- Use benchmarks, scoring tools, and checklists from Security Consensus Operational Readiness Evaluation (SCORE) at http://www.sans.org/score/ for securing desktop systems and servers.
- Download security patches and ensure that patches are kept up-to-date.
- Ensure that only a minimum of services necessary for the system to meet mission requirements are running.
- Avoid the use of trust relationships between systems and use some other method of communication that will meet mission requirements if possible
- Avoid using root when a non-privileged account will meet mission requirements.

12.4 Backups

Mutual Responsibilities

Ensure that any data maintained by each organization is backed up regularly.

12.5 Disposal of IT Equipment

Mutual Responsibilities

Ensure that all IT equipment is sanitized before it is surplused or otherwise disposed.

12.6 Warning Banners

Mutual Responsibilities

Ensure that federally-approved warning banners are used for all government-owned systems.

13 EXTERNAL ACCESS

13.1 Remote Access

Mutual Responsibilities

All remote access users, including Organization A employees, contractors, and other authorized users, shall sign the Organization A Security Rules of Conduct before new remote access accounts are activated.

Organization B Responsibilities

Organization B shall ensure that any remote access is conducted using a service that meets or exceeds the security standards in the Organization A Security Rules of Conduct.

13.2 Wireless Security

Mutual Responsibilities

Comply with NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices at* http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf.

14 COMPLIANCE

Organization A is authorized to temporarily block network access for Organization B if such action is warranted by failure of Organization B to comply with the terms of this Network ISA. Organization A may also temporarily block network access for

Organization B if Organization B does not implement reasonable precautions to prevent the risk of security incidents spreading to multiple systems on the Organization A Network. Non-compliance by either party may lead to termination of the interconnection and contract, if applicable.

15 SIGNATURES

Both parties agree to work together to ensure the joint security of the connected networks and the data they store, process, and transmit, as specified in this Network ISA. Each party certifies that its respective network is designed, managed, and operated in compliance with all relevant federal laws, regulations, and policies (NIST SP 800-47).

We agree to the terms and conditions of this Network ISA.

Organization A Chief Information Officer Officer

_____
(Name)

_____
(Signature) (Date)

Organization B Chief Information

_____
(Name)

_____
(Signature) (Date)

Organization A Senior Information Security Officer

_____
(Name)

_____
(Signature) (Date)

Organization B Information Security Officer

_____
(Name)

_____
(Signature) (Date)

Organization A Information Security Officer

_____
(Name)

_____
(Signature) (Date)

Organization B IT Security Point of Contact

_____
(Name)

_____
(Signature) (Date)

REFERENCES

URLs

1. NIST Special Publications web page. URL: http://csrc.nist.gov/publications/nistpubs/.
2. Tim Grance, Joan Hash, Steven Peck, Jonathan Smith, Karen Korow-Diks. National Institute of Standards and Technology *Security Guide for Interconnecting Information Technology Systems* (NIST Special Publication 800-47, August 2002. URL: http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf.
3. Marianne Swanson, Federal Computer Security Program Managers' Forum Working Group. NIST SP 800-18: *Guide for Developing Security Plans for IT Systems*. December 1998. URL: http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF.
4. Tom Karygiannis, Les Owens. NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices.* November 2002. URL: http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf.
5. SANS Sample Policy: The Third Party Network Connection Agreement. URL: http://www.sans.org/resources/policies/Third_Party_Agreement.pdf.
6. SANS Twenty Most Critical Internet Security Vulnerabilities. URL: http://isc.sans.org/top20.html.
7. Security Consensus Operational Readiness Evaluation (SCORE). URL: http://www.sans.org/score/.

Legislation and Regulations

1. Computer Security Act of 1987 (P.L. 100-235)
2. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems*
3. Federal Information Security Management Act (FISMA) of 2002 [Title X of the Homeland Security Act of 2002 (P.L. 107-296) and Title III of the E-Government Act of 2002 (P.L. 107-347)]
4. Privacy Act of 1974 (5 U.S.C. § 552a)
5. Trade Secrets Act (18 U.S.C. § 1905)
6. Title II of the Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2701-2712).