The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

CCSDS GUIDE FOR SECURE SYSTEM INTERCONNECTION

INFORMATIONAL REPORT

CCSDS 350.4-G-2

GREEN BOOK

April 2019

The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

CCSDS GUIDE FOR SECURE SYSTEM INTERCONNECTION

INFORMATIONAL REPORT

CCSDS 350.4-G-2

GREEN BOOK

April 2019

AUTHORITY

Issue:	Informational Report, Issue 2
Date:	April 2019
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and reflects the consensus of technical panel experts from CCSDS Member Agencies. The procedure for review and authorization of CCSDS Reports is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4).

This document is published and maintained by:

CCSDS Secretariat
National Aeronautics and Space Administration
Washington, DC, USA
Email: secretariat@mailman.ccsds.org

FOREWORD

This document is based upon a United States Government document produced by the National Institute of Standards and Technology (NIST). NIST allows the free use and copying of its documents per the "Use of NIST Information" posted on the NIST web site at http://www.nist.gov/public_affairs/disclaim.htm and reproduced below.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Report is therefore subject to CCSDS document management and change control procedures, which are defined in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be sent to the CCSDS Secretariat at the email address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- China Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- Electronics and Telecommunications Research Institute (ETRI)/Korea.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- Hellenic National Space Committee (HNSC)/Greece.
- Hellenic Space Agency (HSA)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- Mohammed Bin Rashid Space Centre (MBRSC)/United Arab Emirates.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 350.4-G-1	CCSDS Guide for Secure System Interconnection, Informational Report, Issue 1	November 2007	Original issue, superseded
CCSDS 350.4-G-2	CCSDS Guide for Secure System Interconnection, Informational Report, Issue 2	April 2019	Current issue: Annex A and Annex B templates have been simplified to remove redundant explanatory text and to better mark the applicable portions to be completed by each affected organization.

CONTENTS

CONTENTS (continued)

1 INTRODUCTION

1.1 PURPOSE OF THIS RECOMMENDATION

This *CCSDS Guide for Secure System Interconnection* is based on the United States National Institute of Standards and Technology (NIST) *Security Guide for Interconnecting Information Technology Systems* (NIST Special Publication 800-47—reference [1]) that was produced in August 2002.

NIST 800-47 was written to provide *general* guidance to U.S. government agencies for "planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations."

Many organizations using CCSDS recommendations – including commercial enterprises and contractors/suppliers as well as governmental agencies – require such guidance when interconnecting their networks and IT systems to provide cross-support services. For example, ESA may require a connection to NASA/JPL for the use of the Deep Space Network (DSN) to provide full-period mission coverage that might otherwise not be available. Likewise, JAXA might make use of ESA tracking or control stations and would therefore require connectivity between JAXA and ESA networks and systems.

The interconnection of specific agency networks or IT systems is fraught with security implications resulting from varying IT security policies, IT security enforcement, and security control requirements. In the past, the policies, regulations, and memoranda of agreement governing such agency interconnections have been one-of-kind, locally generated, and different between organizations, leading to potential security enforcement issues.

This document has tailored and adapted NIST 800-47 for the space community to provide a CCSDS Guide (Green Book) for secure space agency interconnections.

1.2 SCOPE

This document presents guidelines for interconnecting space agency networks and IT systems, specifically to support secure cross support. However, this document may also be used as a guide for interconnecting organizational networks and IT systems for other purposes as determined to be required by the organizations themselves.

1.3 APPLICABILITY

1.3.1 APPLICABILITY OF THIS RECOMMENDATION

This recommendation is applicable to all organizations with a requirement to interconnect their networks and IT systems with systems owned and operated by other space agency organizations.

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

1.3.2 LIMITS OF APPLICABILITY

The use of this guide is encouraged for IT system and network interconnections between space agencies. However, it may also be used within sectors of a space agency (e.g., NASA/JSC and NASA/JPL, ESA/ESOC and ESA/ESTEC).

It is recognized, however, that many organizations already have interconnected networks and IT systems that use different approaches, and some follow specific procedures to meet unique operational requirements.

This document is intended as guidance and should not be construed as defining the *only* approach possible. It provides a logical framework for organizations that have not previously interconnected IT systems and networks, or are planning new interconnections, and it provides information that may be used to enhance the security of existing interconnections. Organizations are encouraged to tailor the guidelines to meet their specific needs and requirements.

1.4 RATIONALE

Interconnection of individual space agency networks and IT systems to support missions has been difficult to accomplish. Each agency has its own unique security requirements, policies, and enforcement. More often than not, the security requirements, polices, and enforcement will not be uniform. They may employ different access-control policies and enforcement techniques. One may require two-factor authentication to log onto systems while another may allow plain-text passwords. One space agency may segregate mission data systems onto closed, physically segregated networks while others may not enforce such strict separation.

Yet, because of the lack of resources owned by one agency but available from another, network and IT system interconnections must be performed in order to minimize the financial impact to flight missions.

This document addresses the life-cycle-management approach for space agency interconnection of networks and IT systems with an emphasis on security. The four phases of the interconnection life cycle addressed are:

– **Planning the interconnection:** the participating organizations perform preliminary activities; examine all relevant technical, security, and administrative issues; and form an agreement governing the management, operation, and use of the interconnection.

- **Establishing the interconnection:** the organizations develop and execute a plan for establishing the interconnection including implementing, configuring, and testing appropriate security controls.
- **Maintaining the interconnection:** the organizations actively maintain the interconnection after it is established to ensure that it operates properly and securely.
- **Disconnecting the interconnection:** one or all of the interconnected organizations may choose to terminate the interconnection. The termination should be conducted in a planned manner to avoid disrupting the other organization's systems. In response to an emergency, one or all organizations may decide to terminate the interconnection immediately.

This CCSDS document provides recommended steps for completing each phase, emphasizing security measures that should be taken to protect the connected systems and shared data.

This document also contains guides and samples for developing an Interconnection Security Agreement (ISA) and a Memorandum of Understanding/Agreement (MOU/A). The ISA specifies the technical and security requirements of the interconnection, and the MOU/A defines the responsibilities of the participating organizations. Finally, this document contains a guide for developing a System Interconnection Implementation Plan, which defines the process for establishing the interconnection, including scheduling and costs.

1.5 DOCUMENT STRUCTURE

1.5.1 DOCUMENT ORGANIZATION

This document is organized into six sections. Section 1 introduces the document. Section 2 describes the benefits of interconnecting IT systems, identifies the basic components of an interconnection, identifies methods and levels of interconnectivity, and discusses potential risks of interconnecting systems.

Sections 3 through 6 address the interconnection life cycle. Section 3 presents recommended steps for planning a system interconnection. Section 4 provides recommended steps for establishing the interconnection. Section 5 provides recommended steps for maintaining the system interconnection after it is established. Section 6 provides guidelines for terminating the interconnection and restoring it after it is terminated.

Annex A provides a sample template for developing an Interconnection Security Agreement, which documents the technical requirements of the interconnection.

Annex B provides a sample template for developing a Memorandum of Understanding/Agreement, which defines the responsibilities of the participating organizations.

Annex C provides a guide for developing a System Interconnection Implementation Plan, which defines the process of establishing the interconnection.

1.6 DEFINITIONS, NOMENCLATURE, AND CONVENTIONS

1.6.1 DEFINITIONS

Selected terms used in the Recommendation for Secure System Interconnection are defined below. Other terms not defined below may be found in the Security Glossary (reference [4]).

System Interconnection: The direct connection of two or more IT systems for the purpose of sharing data and other information resources.

1.7 REFERENCES

The following publications are referenced in this document. At the time of publication, the editions indicated were valid. All publications are subject to revision, and users of this document are encouraged to investigate the possibility of applying the most recent editions of the publications indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS publications.

[1] *Security Guide for Interconnecting Information Technology Systems*. National Institute of Standards and Technology Special Publication 800-47. Gaithersburg, Maryland: NIST, August 2002.

[2] *Information Technology—Security Techniques—Methodology for IT Security Evaluation*. 2nd ed. International Standard, ISO/IEC 18045:2008. Geneva: ISO, 2008.

[3] *Information Technology—Security Techniques—Information Security Management for Inter-Sector and Inter-Organizational Communications*. 2nd ed. International Standard, ISO/IEC 27010:2015. Geneva: ISO, 2015.

[4] *Information Security Glossary of Terms*. Issue 2. Recommendation for Space Data System Practices (Magenta Book), CCSDS 350.8-M-2. Forthcoming.

[5] *Cross Support Reference Model—Part 1: Space Link Extension Services*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 910.4-B-2. Washington, D.C.: CCSDS, October 2005.

[6] J. Postel and J. Reynolds. *File Transfer Protocol (FTP)*. STD 9. Reston, Virginia: ISOC, October 1985.

[7] C. Rigney, et al. *Remote Authentication Dial In User Service (RADIUS)*. RFC 2865. Reston, Virginia: ISOC, June 2000.

[8] “Kerberos: The Network Authentication Protocol.” Massachusetts Institute of Technology. http://web.mit.edu/Kerberos/. (4/27/2007)

NOTE – Appendix E of reference [1] contains a complete list of references relevant to the development of the original NIST document.

2 BACKGROUND

A system interconnection is defined as the direct connection of two or more IT systems or networks for the purpose of sharing data and other information resources. Through a system interconnection, space agencies can realize significant benefits that include cross support capabilities, access to resources and equipment (e.g., ground systems, relay satellites) not available locally, reduced operating costs, greater functionality, improved efficiency, and centralized access to data. Interconnecting networks and IT systems may also strengthen ties among participating organizations by promoting communication and cooperation.

Space agencies may choose to interconnect their networks or IT systems for a variety of reasons, depending on their needs or mandates. For example, organizations may interconnect their IT systems to:

- provide cross support for each other's missions;
- make use of each other's available resources such as ground systems and tracking stations;
- exchange data and information among selected users;
- provide customized levels of access to proprietary databases;
- collaborate on joint projects;
- provide full-time communications, 24 hours per day, 7 days per week;
- provide online training;
- provide secure storage of critical data and backup files.

A system interconnection has three basic components: two IT systems or networks (System/Network A and System/Network B) and the mechanism by which they are joined (the "pipe" through which data is made available, exchanged, or passed one-way only). The components are shown in figure 2-1. In this document, it is assumed that System A and System B are owned and operated by different organizations. However, nothing in this document precludes the systems or networks from being owned by different parts of the same organization.

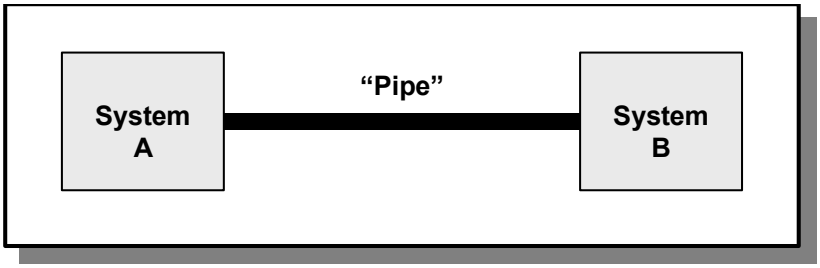

Figure 2-1: Interconnection Components

Organizations can connect their IT systems/networks using a dedicated line that is owned by one of the organizations or is leased from a third party (e.g., an Integrated Services Digital Network [ISDN], E1, E3, T1, or T3 line). The private or leased line is the "pipe" that connects the IT systems.[1] In many cases, because of international boundaries and multiple providers, this solution is expensive but it can provide a high level of security for the interconnected systems because the line may be breached only through a direct physical intrusion.

A less expensive alternative is to connect systems over a public network (e.g., the Internet), using virtual private network (VPN) technology. VPN technology enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them via encryption. This replaces the need to rely on privately owned or leased lines. If VPN technology is not employed, data transmitted over a public network can be intercepted or modified by unauthorized parties. VPNs ensure data confidentiality and integrity over the public networks. Alternately, an organization may pass data over a public network without encryption, and instead rely solely on data authentication if the data is to be publicly available or is of low value. The decision to pass data over a public network should be based on an assessment of the value/sensitivity of the data and the associated risks.

There are varying levels of a system interconnection. As with any form of system access, the extent to which an organization may access data and information resources is dependent on its mission and security needs. Accordingly, some organizations may choose to establish a limited interconnection, whereby users are restricted to a single server, application or file location, with rules governing access. Other space agencies may establish a broader interconnection, enabling users to access multiple mission systems, ground systems, tracking systems, applications, or databases. Still others may establish an interconnection that permits full transparency and access across their respective enterprises.

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

Therefore it is critical that all participating organizations learn as much as possible about the risks associated with the planned or current interconnection and the security controls that they can implement to mitigate those risks. It is also critical that they establish an agreement between themselves regarding the management, operation, and use of the interconnection and that they formally document this agreement. The agreement should be reviewed and approved by the appropriate senior staff from each organization.

[1] In addition to the physical "pipe," other active components such as switches, routers, and firewalls may be required for the connection. Likewise, protocols may also be employed to move data across the connection.

3 PLANNING A SYSTEM INTERCONNECTION

3.1 GENERAL

The process of connecting networks or IT systems should begin with a planning phase in which the participating organizations perform preliminary activities and examine all relevant technical, security, and administrative issues. The purpose of the planning phase is to ensure that the interconnection will operate as efficiently and securely as possible. This section discusses recommended steps for planning a system interconnection, as shown in figure 3-1.

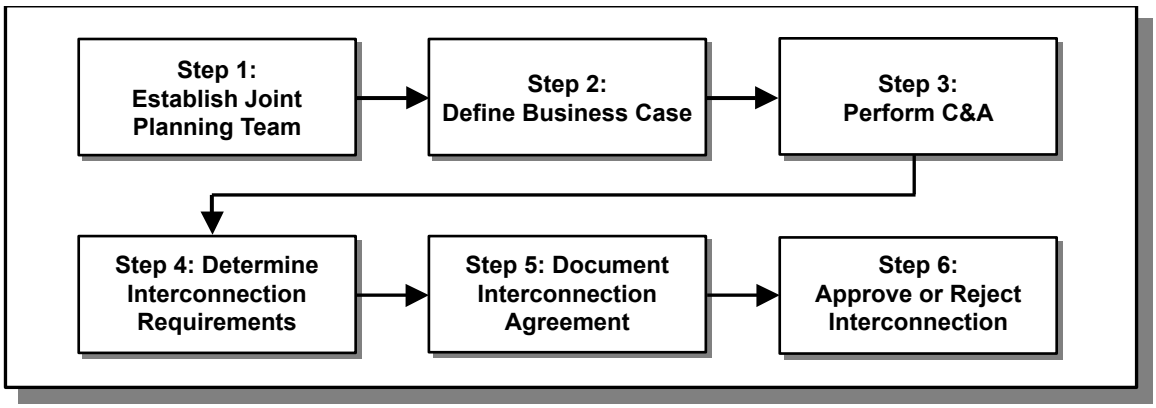

Figure 3-1: Steps to Plan a System Interconnection

3.2 STEP 1: ESTABLISH A JOINT PLANNING TEAM

Each organization is responsible for ensuring the security of its respective systems and data. Essential to this goal is a well-coordinated approach to interconnectivity, including regular communication between the organizations throughout the life cycle of the interconnection. Therefore, the participating space agencies should consider establishing a joint planning team composed of appropriate managerial and technical staff, including program managers, security officers, system administrators, network administrators, and mission and system architects.[2]

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

[2] In some cases, the planning team could comprise a "core" of selected individuals who would consult with functional experts and specialists on an "as-needed" basis during the planning process.

In addition, members of the planning team should coordinate with their colleagues who are responsible for IT capital planning, configuration management, and related activities. In most cases, the interconnection will be a component of each organization's network. By coordinating the interconnection planning with related activities, the organizations can reduce redundancy and promote efficiency.

3.3 STEP 2: DEFINE THE BUSINESS CASE

The interconnecting organizations should work together to define the purpose of the interconnection, determine how it will support their respective mission requirements, and identify potential costs and risks. Defining the *business case* will establish the basis for the interconnection and facilitate the planning process. Factors that should be considered are likely costs (e.g., staffing, equipment, and facilities), expected benefits (e.g., use of limited resources, improved efficiency, centralized access to data), and potential risks (e.g., security, technical, legal, and financial).

As part of this process, the organizations should examine privacy issues related to data that will be exchanged or passed over the interconnection and determine whether such use is restricted under current statutes, regulations, or policies. Examples of data that might be restricted include personal identification information such as names and identity numbers, medical/health data, or confidential business information such as contractor bid rates and trade secrets. Each organization should consult with its privacy officer or legal counsel to determine whether such information may be shared or transferred. Permission to exchange or transfer data should be documented, along with a commitment to protect such data.

Reference [3] discusses policy and requirements considerations regarding identification, marking, and transfer of organization-sensitive data within the context of an information-sharing agreement between multiple organizations.

3.4 STEP 3: PERFORM CERTIFICATION AND ACCREDITATION

Before interconnecting, each organization should ensure that its respective systems are properly certified and accredited in accordance with national or local organizational Certification and Accreditation (C&A) guidelines. Certification involves testing and evaluating the technical and non-technical security features of the systems to determine the extent to which they meet a set of specified security requirements. Accreditation is the official approval by an authorizing official that the system may operate for a specific purpose using a defined set of safeguards at an acceptable level of risk.

The Common Criteria's Common Evaluation Methodology (CEM) is one possible mutual C&A process which could be used among interconnecting space agencies and/or organizations. An international standard (reference [2]), the CEM is the methodology agreed to by a consortium of twenty-four nations that have agreed to recognize each other's security evaluations.

3.5 STEP 4: DETERMINE INTERCONNECTION REQUIREMENTS

The assigned joint planning team should identify and examine all relevant technical, security, and administrative issues surrounding the proposed interconnection. This information may be used to develop an ISA and an MOU/A[3] (or equivalent document[s]).[4] This information may also be used to develop an implementation plan for establishing the interconnection.

The joint planning team should consider the following issues:

- *Level and Method of Interconnection*. Define the level of interconnectivity that will be established between the networks or IT systems, ranging from limited connectivity (limited data exchange) to enterprise-level connectivity (active sharing of data and applications). In addition, describe the method used to connect the systems (dedicated line, VPN, or other).

- *Impact on Existing Infrastructure and Operations*. Determine whether the network or computer infrastructure currently used by the organizations is sufficient to support the interconnection, or whether additional components are required (e.g., communication lines, routers, switches, servers, firewalls, and software). Determine the potential impact that installing and using new components might have on the existing infrastructure. Determine the potential impact the interconnection could have on current operations, including increases in data traffic; new training requirements; and new demands on system administration, security, and maintenance.

- *Hardware Requirements*. Identify hardware that will be needed to support the interconnection, including communications lines, routers, firewalls, hubs, switches, servers, and workstations. Determine whether existing hardware is sufficient, or whether additional components are required. If new hardware is required, select products that ensure secure interoperability.

- *Software Requirements*. Identify software that will be needed to support the interconnection (e.g., software for firewalls, servers, and computer workstations). Determine whether existing software is sufficient, or if additional software is required. If new software is required, select products that ensure secure interoperability.

- *Data Sensitivity*. Identify the sensitivity level of data or information resources that will be made available across the interconnection. Examples of sensitive data may include mission science data, spacecraft or instrument payload commands, financial data, personal information, medical data, and proprietary business data.

- *User Community*. Define the community of users who will access, exchange, or receive data across the interconnection. Determine whether users must possess

[3] Discussions and examples of an ISA and MOU/A are provided in annexes A and B, respectively.
[4] Rather than develop an ISA and MOU/A, the organizations may choose to incorporate this information into a formal contract, especially if the interconnection is to be established between a governmental agency and a commercial organization.

certain characteristics corresponding to data sensitivity levels and whether background checks and security clearances are required.[5]

– *Services and Applications*. Identify the information services that will be provided over the interconnection by each organization and the applications associated with those services. Examples include SLE (reference [5]), FTP (reference [6]), RADIUS (reference [7]), Kerberos (reference [8]), database query, file query, email, and general computational services.

– *Security Controls*. Identify security controls that will be implemented to protect the confidentiality, integrity, and availability of the connected systems and the data that will pass between them. Controls can be selected from the examples provided in section 4 or from other sources.

– *Segregation of Duties*. Determine whether the management or execution of certain duties should be divided between two or more individuals. Examples of duties that might be segregated include auditing, managing user profiles, and maintaining equipment. Segregation of duties reduces the risk that a single individual could cause harm to the connected systems and data, either accidentally or deliberately.

– *Incident Reporting and Response*. Establish procedures to report and respond to anomalous and suspicious activity that is detected by either technology or staff. Determine when and how to notify each other about security incidents that could affect the interconnection or associated data storage (e.g., by spreading through other means). Identify the types of information that will be reported, including the cause of the incident, affected data or programs, and actual or potential impact. In addition, identify types of incidents that require a coordinated response, and determine how to coordinate response activities. It might be appropriate to develop a joint incident response plan for this purpose.

– *Contingency Planning*. Each organization should have a contingency plan to respond to and recover from disasters and other disruptive contingencies that could affect its IT system, ranging from the failure of system components to the loss of computing facilities. Determine how to notify each other of such contingencies, the extent to which the interconnected organizations will assist each other, and the terms under which assistance will be provided. Emergency Points Of Contact (POCs) should be identified and exchanged. Determine whether to incorporate redundancy into components supporting the interconnection, including redundant interconnection points, and how to retrieve data backups. Coordinate disaster response training, testing, and exercises.

[5] When an interconnection is to be established between organizations representing different governments, each party should be cognizant of the other's rules governing background checks and security clearances.

- *Data Element Naming and Ownership*. Determine whether the data element naming schemes used by the participating organizations are compatible, or whether new databases must be normalized so the organizations can use data passed over the interconnection. In addition, determine whether ownership of data is transferred from the transmitting organization to the receiving organization, or whether the transmitting organization retains ownership and the receiver becomes the custodian. As part of this effort, determine how transferred data will be stored, whether data may be reused, and how data will be destroyed. In addition, determine how to identify and resolve potential data element naming conflicts.

- *Data Backup*. Determine whether data or information that is passed across the interconnection must be backed up and stored. If backups are required, identify the types of data that will be backed up, how frequently backups will be conducted (daily, weekly, or monthly), and whether backups will be performed by one or multiple organizations. Also, determine how to perform backups, and how to link backups to contingency plan procedures. Critical data should be backed up regularly, stored in a secure off-site location to prevent loss or damage, and retained for a period approved by all participating organizations. The use of encryption to protect against loss of backup media while in transport to off-site locations should be considered. Similarly, audit logs should be copied, stored in a secure location, and retained for a period approved by all interconnected organizations.

- *Change Management*. Determine how to coordinate the planning, design, and implementation of changes that could affect the connected systems or data, such as upgrading hardware or software, or adding services. Establish a joint change management board to review proposed changes to the interconnection, as appropriate.

- *Rules of Behavior*. Develop rules of behavior that clearly delineate the responsibilities and expected behavior of all personnel who will be authorized to access the interconnection. The rules should be in writing, and they should state the consequences of inconsistent behavior or noncompliance. The rules should be covered in a security training and awareness program.

- *Security Training and Awareness*. Define a security training and awareness program for all authorized personnel who will be involved in managing, using, and/or operating the interconnection. The program may be incorporated into current security training and awareness activities.

- *Roles and Responsibilities*. Identify personnel who will be responsible for establishing, maintaining, or managing the interconnection, including managers, system administrators, application designers, auditors, security staff, and other specialists as needed.

- *Scheduling*. Develop a preliminary schedule for all activities involved in planning, establishing, and maintaining the interconnection. Also, determine the schedule and conditions for terminating or reauthorizing the interconnection.

– *Costs and Budgeting*. Identify the expected costs required to plan, establish, and maintain the interconnection. Determine how costs will be apportioned between the organizations.

3.6 STEP 5: DOCUMENT INTERCONNECTION AGREEMENT

The joint planning team should document an agreement governing the interconnection and the terms under which the organizations will abide by the agreement, based on the team's review of all relevant technical, security, and administrative issues (see 3.5, above). Two documents may be developed: an ISA and an MOU/A.[6] An ISA development guide and sample are provided in annex A and an MOU/A development guide and sample are provided in annex B.

3.7 STEP 6: APPROVE OR REJECT SYSTEM INTERCONNECTION

The joint planning team should submit the ISA and the MOU/A to the authorizing management official of each participating organization, requesting approval for the interconnection. Upon receipt, the authorizing official should review the ISA, the MOU/A, and any other relevant documentation or activities, including those addressed in section 4.

If the authorizing officials accept the ISA and the MOU/A, they should sign and date the documents, thereby approving the interconnection.

One or more of the authorizing officials may decide to grant an *interim approval*. Interim approval may be granted if the planned interconnection does not meet all of the requirements stated in the ISA, but mission criticality requires that the interconnection must be established. The authorizing official(s) should document the tasks that must be completed before full approval will be granted.

If one or more authorizing officials reject the interconnection, the reasons for rejecting the planned interconnection and proposed remediation should be documented. The authorizing officials also should meet with the joint planning team to discuss and agree on the proposed solutions and timelines for correcting specified deficiencies, so approval may be granted.

[6] In some cases, the organizations may decide to use already established procedures for documenting the agreement, in lieu of an ISA and MOU/A.

4 ESTABLISHING A SYSTEM INTERCONNECTION

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

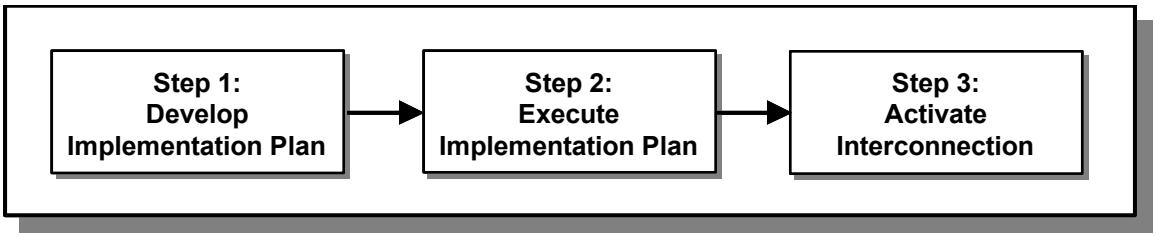

Figure 4-1: Steps to Establish a System Interconnection

4.1 STEP 1: DEVELOP AN IMPLEMENTATION PLAN

The joint planning team should develop a System Interconnection Implementation Plan. The purpose of the plan is to centralize all aspects of the interconnection effort in one document and to clarify how technical requirements specified in the ISA will be implemented.

At a minimum, the implementation plan should

- describe the networks and IT systems that will be connected;
- identify the sensitivity of data that will be made available across the interconnection;
- identify personnel who will establish and maintain the interconnection, and specify their responsibilities;
- identify implementation tasks and procedures;
- identify and describe security controls that will be used to protect the confidentiality, integrity, and availability of the connected systems and data (see 4.2.1 for sample security controls);
- provide test procedures and measurement criteria to ensure the interconnection operates properly and securely;
- specify training requirements for users, including a training schedule;
- cite or include all relevant documentation, such as system security plans, design specifications, and standard operating procedures.

A guide for developing a System Interconnection Implementation Plan is provided in annex C.

4.2 STEP 2: EXECUTE THE IMPLEMENTATION PLAN

The implementation plan should be reviewed and approved by senior members of the planning team. A list of recommended tasks for establishing an interconnection is provided below. Detailed procedures associated with each task should be described.

4.2.1 SUBSTEP 1: IMPLEMENT OR CONFIGURE SECURITY CONTROLS

Security controls must be implemented, or existing controls configured, as specified in the ISA and the implementation plan. The security controls may be implemented as separate, discrete systems. Alternatively, a firewall may be capable of providing many of the required security controls in a single device. Security controls may include the following:

- *Firewalls*. Firewalls determine whether data packets are permitted into or out of a network, and they restrict access to specific resources. Install firewalls to protect internal networks and other resources from unauthorized access across the interconnection, or configure existing firewalls accordingly. If the interconnection involves the use of servers, they may be hosted in a separately protected "demilitarized zone" (DMZ). A firewall may also be capable of providing other security controls (as listed below) such as intrusion detection/prevention, auditing, identification, authentication, access controls, virus scanning, and encryption services.

- *Intrusion Detection and Prevention*. An IDS detects security breaches by looking for anomalies in normal activities, and/or by looking for patterns of activity that are associated with intrusions or insider misuse. A combination of network-based and host-based IDSes may be used, if appropriate. Alert mechanisms should be configured to notify system administrators or security officers when intrusions or unusual activities are detected. An Intrusion Prevention System (IPS) not only detects security breaches but attempts to prevent their occurrence, analogous to anti-virus software which helps prevent the viral infection of a system. Organizations may elect to deploy IPSes in addition to, or in replacement of IDSes.

- *Auditing*. Install or configure mechanisms to record activities occurring across the interconnection, including application processes and user activities. Activities that should be recorded include event type, date and time of event, user identification, workstation identification, the success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs should have read-only access, and only authorized personnel should have access to the logs. Logs should be stored in a secure location to protect against theft and damage, and they should be retained for a period approved by all affected organizations.

- *Identification and Authentication*. Identification and authentication is used to prevent unauthorized personnel from entering an IT system. Implement strong mechanisms to identify and authenticate users to ensure that they are authorized to access the interconnection. Mechanisms that may be used include user identification and passwords, digital certificates, authentication tokens, biometrics, and smart cards.

The transmission of unencrypted passwords over a network is highly discouraged. If passwords are used, they should be at least eight characters long, have a mixture of alphabetic and numeric characters, and be changed at predetermined intervals. Depending on data sensitivity, organizations may permit users to access the interconnection after they have been authenticated to their local domain, reducing the need for multiple passwords or other mechanisms.

– *Logical Access Controls*. Logical access controls are mechanisms used to designate users who have access to system resources and the types of transactions and functions they are permitted to perform. Access Control Lists (ACLs) and access rules should be used to specify the access privileges of authorized personnel, including the level of access and the types of transactions and functions that are permitted (e.g., read, write, execute, delete, create, and search). Access rules must be configured to grant appropriate access privileges to authorized personnel based on their roles or job functions. Only system administrators should have access to the controls.

– *Virus Scanning*. Data and information that pass from one IT system to another should be scanned with antivirus software to detect and eliminate malicious code, including viruses, worms, and Trojan horses. Antivirus software must be installed on all servers and computer workstations linked to the interconnection. Firewalls may also be used with automated virus scanning technology incorporated. The software must be updated automatically and maintained in accordance with current virus definitions.

– *Encryption*. Encryption is used to ensure data cannot be read or modified by unauthorized users. When used properly, encryption will protect the confidentiality and integrity of data during transmission and storage, and it may also be used for authentication and non-repudiation. Encryption may be implemented in devices such as routers, switches, firewalls, servers, and computer workstations. Devices must be configured to apply the appropriate level of encryption required for data that passes over the interconnection. If required, encryption mechanisms (e.g., digital signatures) should be implemented to authenticate users to the interconnection and to shared applications, and to provide non-repudiation.

– *Physical and Environmental Security*. Hardware and software supporting the interconnection, including interconnection points, must be placed in a secure location protected from unauthorized access, interference, and damage. Environmental controls must be in place to protect against hazards such as fire, water, and excessive heat and humidity. In addition, computer workstations should be placed in secure areas to protect them from damage, loss, theft, or unauthorized physical access. Access badges, cipher locks, or biometric devices should be considered to control access to secure areas, and, biometric devices may be used to prevent unauthorized use of workstations.

4.2.2 SUBSTEP 2: INSTALL OR CONFIGURE HARDWARE AND SOFTWARE

After security controls are installed or configured, it may be necessary to install new hardware and software to establish the interconnection, or to configure existing hardware and software for this purpose, if appropriate. Hardware and software must be placed in secure areas that are configured with proper environmental controls.

4.2.3 SUBSTEP 3: INTEGRATE APPLICATIONS

Applications or protocols for services that are provided across the interconnection must be integrated. Examples include SLE, database applications, email, Web browsers, application servers, authentication servers, domain servers, development tools, editing programs, and communications programs. If using Web-based applications, the possible security ramifications regarding the use of Java, JavaScript, ActiveX, and cookies should be considered.

4.2.4 SUBSTEP 4: CONDUCT OPERATIONAL AND SECURITY TESTING

A series of tests must be conducted and documented to ensure equipment operates properly and that there are no obvious ways for unauthorized users to circumvent or defeat security controls.[7] The interface must be tested between applications across the interconnection, and data traffic must be simulated at planned activity levels to verify correct translation at the receiving end(s). In addition, security controls must be tested under realistic conditions. If possible, testing should be conducted in an isolated, non-operational environment to avoid affecting other systems.

4.2.5 SUBSTEP 5: CONDUCT SECURITY TRAINING AND AWARENESS

Security training and awareness should be conducted for all authorized personnel who will be involved in managing, using, and/or operating the interconnection. Training and awareness should be provided for new users, and a refresher training should be provided for all users periodically.

4.2.6 SUBSTEP 6: UPDATE SYSTEM SECURITY PLANS

The organizations involved should update their system security plans and related documents to reflect the changed security environment in which their respective system operates as a result of the interconnection. In addition, each organization involved should consider conducting mutual reviews of the sections of the updated plans that are relevant to the

[7] Operational and security testing may be performed as part of recertification and reaccreditation discussed in 4.2.7.

interconnection. The details for conducting a mutual review should be addressed in the MOU/A.

It is recommended that the security plans include the following information regarding the system interconnection (and other interconnections, if appropriate):

- names of interconnected systems;
- organization owning the other systems;
- type of interconnection;
- short discussion of major concerns or considerations in determining interconnection;
- name and title of authorizing management official(s);
- date of authorization;
- system of record, if applicable;
- sensitivity level of each system;
- interaction among systems;
- hardware inventory;
- software inventory;
- security concerns and rules of behavior governing the interconnection.

4.2.7 SUBSTEP 7: PERFORM RECERTIFICATION AND REACCREDITATION

Establishing an interconnection may represent a significant change to the connected systems. Therefore, each organization should consider recertifying and reaccrediting its respective system(s) to verify that security protection remains acceptable. Recertification and reaccreditation involve the same activities described in 3.4.

4.3 STEP 3: ACTIVATE THE INTERCONNECTION

The interconnection must be activated in accordance with the prescribed guidelines so it may be used by all organizations involved. It is recommended that one or more of the organizations test, exercise, and closely monitor the interconnection for a period of at least three months to ensure it operates properly and securely before going operational. Audit logs must be analyzed carefully and frequently, and the types of assistance requested by users should be monitored. Any weaknesses or problems that occur should be documented and corrected.

5 MAINTAINING A SYSTEM INTERCONNECTION

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

- maintain clear lines of communication;
- maintain equipment;
- manage user profiles;
- conduct security reviews;
- analyze audit logs;
- report and respond to security incidents;
- coordinate contingency planning activities;
- perform change management;
- maintain system security plans.

5.1 MAINTAIN CLEAR LINES OF COMMUNICATION

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

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

- initial agreements and changes to agreements;
- changes in designated management and technical personnel;
- activities related to establishing and maintaining the interconnection;
- change management activities that could affect the interconnection;
- security incidents that could affect the connected systems and data;
- disasters and other contingencies that disrupt one or both of the connected systems;
- termination of the interconnection;
- planned restoration of the interconnection.

5.2 MAINTAIN EQUIPMENT

The participating organizations should agree on who will maintain the equipment used to operate the interconnection. Equipment should be maintained at regular service intervals and in accordance with manufacturer specifications. Only authorized personnel should be allowed to service and repair equipment. All maintenance activities and corrective actions should be documented, and the records should be stored in a secure location. Organizations should notify each other before performing maintenance activities, including scheduled outages.

5.3 MANAGE USER PROFILES

If a user resigns or changes job responsibilities, the appropriate organization should update the user's profile to prevent access to data or information that is no longer appropriate. Procedures should be established for investigating, disabling, and terminating access to users who do not actively access the interconnection over a specific period of time.

5.4 CONDUCT SECURITY REVIEWS

All of the participating organizations should review the security controls for the interconnection at least annually or whenever a significant change occurs to ensure they are operating properly and are providing appropriate levels of protection. It is suggested that penetration tests by one or more participating organizations also be conducted. This testing must be coordinated so that the other organizations participating in the interconnection do not think they are under attack.

Security reviews may be conducted by designated audit authorities of one or all participating organizations, or by an independent third party. All participating organizations should agree on the rigor and frequency of reviews as well as a reporting process. The results of security reviews should be examined to identify areas requiring attention. Security risks or problems should be corrected or addressed in a timely manner. Corrective actions should be documented, and the records should be stored in a secure location.

5.5 ANALYZE AUDIT LOGS

One or all of the participating organizations should analyze audit logs at predetermined intervals to detect and track unusual or suspicious activities across the interconnection that might indicate intrusions or internal misuse. Automated tools should be used to scan for anomalies, unusual patterns, and known attack signatures, and to alert a system administrator if a threat is detected. In addition, experienced system administrators should review the logs periodically to detect patterns of suspicious activity that scanning tools might not recognize. Audit logs should be retained for a period approved by all participating organizations.

5.6 REPORT AND RESPOND TO SECURITY INCIDENTS

The space agencies should notify each other of intrusions, attacks, or internal misuse, so the other organization(s) can take steps to determine whether its systems have been compromised. All agencies should take the appropriate steps to isolate and respond to such incidents, in accordance with their respective incident response procedures. Actions that may be taken include shutting down a computer, disabling an account, reconfiguring a router or firewall, and shutting down a network pipe. If the incident involves personnel from one or more organizations, disciplinary actions may be required.

In some cases, all of the participating agencies should coordinate their incident response activities, especially if a major security breach occurs. If the incident was an attack or an intrusion attempt, the appropriate law enforcement authorities should be notified, and all attempts should be made to preserve evidence. All security incidents, along with the reporting and response actions taken, should be documented.

5.7 COORDINATE CONTINGENCY PLANNING ACTIVITIES

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

5.8 PERFORM CHANGE MANAGEMENT

Each organization should establish a Change Control Board (CCB) to review and approve planned changes to its respective system, such as upgrading software or adding services. If a planned change specifically affects the interconnection, the organizations should convene a joint Control Board or similar body to review and approve the change.

Upgrades or modifications should be based on the security requirements specified in the ISA and a determination that the change will not adversely affect the interconnection. Changes should be tested in an isolated, non-operational environment to avoid affecting the interconnected systems as much as possible. Space agencies should consider blocking all changes during critical mission phases if the interconnection provides inter-agency cross support. If changes are allowed, all interconnected organizations' operations teams should be notified in advance, and they should be involved in scheduling this process.

In most cases, such changes are designed to improve the operation and security of the interconnection, such as by adding new functions, improving user interfaces, and eliminating (or mitigating) known vulnerabilities.

5.9 MAINTAIN SYSTEM SECURITY PLANS

The organizations should update their system security plans and other relevant documentation annually, at a minimum. Such plans and other relevant documentation should also be updated whenever there is a significant change to the IT systems or the interconnection.

6 DISCONNECTING A SYSTEM INTERCONNECTION

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

6.1 PLANNED DISCONNECTION

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

6.2 EMERGENCY DISCONNECTION

If one or more organizations detect an attack, intrusion attempt, or other contingency that exploits or jeopardizes the connected systems or their data, it might be necessary to terminate the interconnection abruptly without providing written notice to the other agencies. This extraordinary measure should be taken only in extreme circumstances and only after consultation with the appropriate technical staff and approval by senior management.[8]

The system owner or designee should immediately notify the other organizations' emergency contacts and receive confirmation of the notification. All agencies should work together to isolate and investigate the incident, including conducting a damage assessment and reviewing audit logs and security controls in accordance with incident response procedures. If the incident was an attack or an intrusion attempt, the pertinent law enforcement authorities should be notified, and all attempts should be made to preserve evidence.

The initiating organization should provide a written report to the other agencies in a timely manner (e.g., within five days). The report should describe the nature of the incident, explain why the interconnection was terminated, describe how the interconnection was terminated, and identify actions taken to isolate and investigate the incident. In addition, the report may specify when and under what conditions the interconnection may be restored.

[8] Each organization should consult with its legal counsel well in advance of a potential emergency disconnection to address issues related to liability, investigation, and evidence preservation.

6.3 RESTORATION OF INTERCONNECTION

The affected organizations may choose to restore the system interconnection after it has been terminated. If the interconnection was terminated because of an attack, intrusion, or other contingency, all agencies should implement the appropriate countermeasures to prevent a recurrence of the problem. They should also modify the ISA and MOU/A to address issues requiring attention, if necessary.

ANNEX A

INTERCONNECTION SECURITY AGREEMENT

The organizations that own and operate the connected IT systems should develop an ISA (or an equivalent document) to document the technical requirements of the interconnection. The intent of the ISA is to document and formalize the interconnection arrangements and to specify any details that may be required to provide overall security safeguards for the systems being interconnected. General guidance regarding the contents of an ISA is provided below; however, an ISA may be tailored by mutual consent of the participating organizations. The ISA also supports an MOU/A between the organizations (see annex B). A sample ISA template is provided below.

1 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to define the Interconnection Security Agreement (ISA) between <Organization_A> and <Organization_B> in the context of <Mission>.

This document is written following CCSDS guidelines about secure system interconnection (see reference [RD-1]), merging the Interconnection Security Agreement and the Memorandum of Understanding into a single document.

This document:

– Recalls the background information related to the design of the interconnection;

– Defines the high-level considerations for ensuring the security of the interconnected systems.

1.2 SCOPE

The Interconnection Security Agreement (ISA) covers interfaces described in OICD (reference [AD-2]).

1.3 APPLICABLE DOCUMENTS

AD-1	<Reference>	<System Requirements applicable to Mission (SRD)>
AD-2	<Reference>	<OICD>
AD-3	<Reference>	<ICD>

1.4 REFERENCE DOCUMENTS

RD-1	CCSDS 350.4-G-2	CCSDS Guide for Secure System Interconnection
RD-2	<Reference>	<Organization_A's security policy>
RD-3	<Reference>	<Organization_A's security governance organization>
RD-4	<Reference>	<Organization_A's security requirements for operations>
RD-5	<Reference>	<Organization_A's security requirements for security incident management>
RD-6	<Reference>	<Organization_A's procedure for security incident handling>
RD-7	<Reference>	<Organization_A's data classification guideline>
RD-8	<Reference>	<Organization_B's security policy>
RD-9	<Reference>	<Organization_B's security governance organization>
RD-10	<Reference>	<Organization_B's security requirements for operations>
RD-11	<Reference>	<Organization_B's security requirements for security incident management>
RD-12	<Reference>	<Organization_B's procedure for security incident handling>
RD-13	<Reference>	<Organization_B's data classification guideline>

1.5 DOCUMENT STRUCTURE

Section 1 General information (this section)

Section 2 Provides the content of the Interconnection Security Agreement including: background information, security considerations, operations nominal and contingency scenarios, and agreement timeline.

Section 3 Provides topological drawings.

Section 4 Establishes the official and signed commitment to the Interconnection Security Agreement from both organizations' representatives.

2 INTERCONNECTION SECURITY AGREEMENT

2.1 INTRODUCTION

2.1.1 ORGANIZATIONS & SYSTEMS

This Interconnection Security Agreement (ISA) is concluded between <Organization_A> and <Organization_B> for the interconnection of:

– <Organization_A's system name>, operated by <Organization_A>, and

– <Organization_B's system name>, operated by <Organization_B>.

The expected benefits from this agreement are:

a) to ensure that adequate security safeguards are implemented to minimize security risks;

b) to establish the related joint operations scenarios and run them efficiently; and,

c) to maximize services provided by both organizations.

2.1.2 HIERARCHY OF AGREEMENTS

This agreement does not supersede any previous agreement:

– Between <Organization_A> and <Organization_B>;

– Nor between <Organization_A> and another organization;

– Nor between <Organization_B> and another organization.

2.1.3 DEFINITIONS

This subsection provides definition of terms and concepts used throughout this document. The definitions given in reference [RD-1] are considered agreed by both organizations, and shall be retained as applicable unless superseded by any additional definitions agreed upon in this document.

For this specific document, no additional definitions are provided.

2.2 BACKGROUND

2.2.1 DATA FLOWS AND SENSITIVITY LEVELS

As per reference [AD-3], data flows covered by this agreement are the following:

Source	Destination	Protocol	Data content	Classification
<source>	<destination>	<protocols>	<data>	<classification>
<source>	<destination>	<protocols>	<data>	<classification>

2.2.2 SECURITY ZONES MAPPING

<Organization_A> security zones (as per reference [RD-4]):

The following network types are identified:

– <Organization_A network name> is <Organization_A network type>.

– <Organization_A network name> is <Organization_A network type>.

– <Organization_A network name> is <Organization_A network type>.

– <Organization_B> security zones (as per reference [RD-10]):

The following network types are identified:

– <Organization_B network name> is <Organization_B network type>.

– <Organization_B network name> is <Organization_B network type>.

– <Organization_B network name> is <Organization_B network type>.

Mapping:

<Organization_A> Security Zones	**<Organization_B> Security Zones**
<Organization_A network type>	<Organization_B network type>
<Organization_A network type>	<Organization_B network type>
<Organization_A network type>	<Organization_B network type>

2.3 INTERCONNECTION SECURITY

2.3.1 STATEMENT OF REQUIREMENTS

The formal requirements for building an interconnection between <Organization_A's system name> owned by <Organization_A> and <Organization_B's system name> owned by <Organization_B> are defined in reference [AD-1] as:

– [Requirement ID],

– [Requirement ID],

– [Requirement ID].

The formal requirements for defining a security agreement about this interconnection are defined in reference [AD-1] as:

– [Requirement ID],

– [Requirement ID],

– [Requirement ID].

2.3.2 SYSTEM SECURITY CONSIDERATIONS

2.3.2.1 General Information/Data Description

The interconnection between <Organization_A's system name> and <Organization_B's system name> is a <two-way/single-way> path.

The security of the information being passed on this interconnection is protected through the following methods:

– <WAN link protection: e.g., dedicated leased line, MPLS, IP-VPN, end-to-end ciphered tunnel, etc.>

– <Firewall: e.g., stateful inspection, filtering policy, etc.>

– <Monitoring systems: e.g., intrusion detection and prevention system, centralized logging, event correlation, Security Event Management, data leak prevention, etc.>

– <Ciphered protocols: e.g., SSH/SFTP/FTPS/HTTPS, etc.>

– <Application-layer filtering: e.g., application proxies, application firewall, etc.>

– <User authentication>: e.g., Active Directory, RADIUS, token, etc.>

2.3.2.2 Resources and Information Security

Resources belonging to <Organization_A> and <Organization_B> have to be protected from sensitive information exposure and disclosure, security bypass, unauthorized access, and denial of service.

Measures are taken to prevent malicious exploitation of network, applications, and systems vulnerabilities.

2.3.2.3 Trusted Behavior Expectations

The agreement between <Organization_A> and <Organization_B> is based on the assumption of trust between the organizations. That means that system, network, and security administrators and operators from both organizations are expected to take all actions necessary to protect each other's data and systems.

Planned system outages that will affect this interconnection shall be coordinated sufficiently in advance to allow for the exercise of contingency plans as required. Unplanned outages shall be reported to both organizations, or delegated contractor(s), as soon as possible, through the system points of contact identified in OICD (reference [AD-2]).

Both organizations agree to share proposed changes and the implementation schedule for such changes related to the interface should they be expected to impact the other partner. Both organizations should explain the potential impacts and ensure that such changes are consistent with this agreement.

2.3.2.4 Formal Security Policy

The security policy applicable to <Organization_A> operational systems (reference [RD-2]) is organized in normative documents traceable to <standard>, one of them being dedicated to Information Systems Operations Management (reference [RD-4]).

The security policy applicable to <Organization_B> operational systems (reference [RD-8]) is organized in normative documents traceable to <standard>, one of them being dedicated to Information Systems Operations Management (reference [RD-10]).

2.3.2.5 Data Sensitivity

The following equivalence matrix is established between the classification schemes implemented in <Organization_A> (see reference [RD-7]) and in <Organization_B> (see reference [RD-13]):

Table 2-1: Equivalence between <Organization_A> and <Organization_B> Classification Scheme

<Organization_A> Classification	<Organization_B> Classification
<Organization_A Classification Level>	<Organization_B Classification Level>
<Organization_A Classification Level>	<Organization_B Classification Level>
<Organization_A Classification Level>	<Organization_B Classification Level>
<Organization_A Classification Level>	<Organization_B Classification Level>

The sensitivity of data exchanged between <Organization_A> and <Organization_B> is of the following level, taking into consideration that "inside" refers here below to the <Mission> context and not to the organization context:

– <Organization_A Classification Level> when handled inside <Organization_A> perimeter;

– <Organization_B Classification Level> when handled inside <Organization_B> perimeter;

The creation, processing and exchange of data related to security incidents shall be handled by both organizations on a Need-to-Know and Least Privilege basis, and by using the appropriate encryption methods for exchanging sensitive documents or email attachments highlighting weaknesses or vulnerabilities of the interconnection. This shall be achieved using <Technology agreed between organizations, e.g., encryption tool>.

2.3.2.6 Security Incident Management and Reporting

Security and incidents are jointly managed by <Organization_A> and <Organization_B> in order to prevent and contain impacts.

Security Incident Handling in <Organization_A> is required as per reference [RD-5] and performed as per reference [RD-6]. Security Incident Handling in <Organization_B> is required as per reference [RD-11] and performed as per reference [RD-12].

<Organization_A> and <Organization_B> will notify each other for a security incident immediately after the detection, via the agreed points of contact listed below. A security board will be held as needed.

Table 2-2: Security Incident Points of Contact

Role	<Organization_A>	<Organization_B>
24h/7d Point of Contact	<Organization_A 24h/7d contact details>	<Organization_B 24h/7d contact details>
Incident Response Team	<Organization_A Incident Response Team contact details>	<Organization_B Incident Response Team contact details>
Security Officer	<Organization_A Security Officer contact details>	<Organization_B Security Officer contact details>

2.3.2.7 Audit Trail Responsibilities

Both organizations are responsible for recording user activities related to the interconnection. Recorded activities shall include event type, date and time of the event, user identification, equipment identification, success or failure of access attempts, and security actions taken in response. Audit logs will be retained for <*X* months>.

3 TOPOLOGICAL DRAWINGS

3.1 GENERAL

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:

- all communications links, paths, circuits, and other components used for the interconnection, from <Organization A's system(s)> to <Organization B's system(s)>;
- the logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations).

3.2 LOGICAL ARCHITECTURE

<Network logical architecture figure (e.g., Visio file)>

Figure 3-1: Interconnection Network Logical Diagram

3.3 PHYSICAL ARCHITECTURE

<Network physical architecture figure (e.g., Visio file)>

Figure 3-2: Interconnection Network Physical Diagram

3.4 AGREEMENT TIMELINE

3.4.1 APPLICABILITY

This ISA is valid for the duration of <Mission>.

3.4.2 REVISIONS

This Interconnection Agreement is to be reviewed at least <once per year>, according to the agreed process and procedure between the parties.

If deemed appropriate, ad hoc revisions can be performed as well at the request of either party.

3.4.3 TERMINATION

This Interconnection Agreement ends automatically <at the last day of Mission/after *X* years>.

If deemed appropriate, either party can terminate the Interconnection Agreement in accordance with the process and procedure both parties have agreed upon.

In case of security incidents, either party can decide immediately to reinforce communication restrictions or cut all connectivity between the networks that are the subject of this Interconnection Agreement. In this case, the incident notification, escalation, and handling procedures that are agreed upon between the parties are applicable.

Termination of this Interconnection Agreement does not terminate any related agreements regarding the handling and protection of intellectual property (IP) and/or proprietary data used by either party as part of this Interconnection Agreement.

4 SIGNATORY AUTHORITY

I have read and understood the terms of this Interconnection Security Agreement.

As a system owner I agree to collaborate to ensure the joint security of the interconnected systems and the data they store, process, and transmit. I will ensure compliance with the requirements documented herein.

I understand that non-compliance on the part of either <Organization_A> or <Organization_B> or its users or contractors with regards to <Organization_A> (reference [RD-2]) and <Organization_B> security policies (reference [RD-8]) explained herein may result in the immediate termination of this agreement.

This agreement is valid for the period defined in 3.1. It shall be reviewed as per defined in 3.2 and can be terminated as per defined in 3.3.

(Signature)	(Date)	(Signature)	(Date)
<Organization_A System Owner name>		<Organization_B System Owner name>	
<Organization_A System Owner title>		<Organization_B System Owner title>	

(Signature)	(Date)	(Signature)	(Date)
<Organization_A Security Rep. name>		<Organization_B Security Rep. name>	
<Organization_A Security Rep. title>		<Organization_B Security Rep. title>	

ANNEX B

MEMORANDUM OF UNDERSTANDING/AGREEMENT

The organizations that own and operate the connected systems should establish an MOU/A (or an equivalent document) that defines the responsibilities of all organizations in establishing, operating, and securing the interconnection. This management document should not contain technical details of the interconnection. Those details should be addressed separately in the ISA (see annex A).

An MOU/A development guide is provided below, although organizations may use their own MOU/A format, if appropriate. A sample MOU/A template is attached at the end of this annex.

1 SUPERSESSION

This agreement supersedes: <Document title and date>

2 INTRODUCTION

The purpose of this memorandum is to establish a management agreement between <Organization_A> and <Organization_B> regarding the development, management, operation, and security of a connection between <Organization_A's system name>, owned by <Organization_A>, and <Organization_B's system name>, owned by <Organization_B>. This agreement will govern the relationship between <Organization_A> and <Organization_B>, including designated managerial and technical staff, in the absence of a common management authority.

3 AUTHORITY

Relevant legislative, regulatory, or policy authorities on which the MOU/A is based must be identified.

The authority for this agreement is based on <Proclamation> issued by the Directors of <Organization_A> and <Organization_B> on <date>.

4 BACKGROUND

The networks and IT systems that will be connected; the data that will be shared, exchanged, or passed one-way across the interconnection; and the business purpose for the interconnection should be described.

It is the intent of both organizations to agree to interconnect the following information technology (IT) systems to exchange data between <Organization_A system> and <Organization_B system>. <Organization_A> requires the use of <Organization_B data>, and <Organization_B> requires the use of <Organization_A data>, as approved and directed in <Proclamation>. The expected benefit of the interconnection is to expedite the processing of data associated with <Project> within prescribed timelines.

Each IT system is described below:

– <Organization_A's system name>
  - Function
  - Location
  - Description of data, including sensitivity

– <Organization_B's system name>
  - Function
  - Location
  - Description of data, including sensitivity

5 COMMUNICATIONS

Frequent formal communications are essential to ensure the successful management and operation of the interconnection. The agencies agree to maintain open lines of communication between designated staff at both the managerial and technical levels. All communications described herein must be conducted in writing unless otherwise noted.

The owners of <Organization_A's system name> and <Organization_B's system name> agree to designate and provide contact information for technical leads for their respective system, and to facilitate direct contact between technical leads to support the management and operation of the interconnection. To safeguard the confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit, the agencies agree to provide notice of specific events within the time frames indicated below:

– **Security Incidents**: Technical staff will immediately notify their designated counterparts by telephone or email when a security incident(s) is detected, so the other organization may take steps to determine whether its system has been compromised and to take the appropriate security precautions. The system owner will receive formal notification in writing within five (5) business days after detection of the incident(s).

– **Disasters and Other Contingencies**: Technical staff will immediately notify their designated counterparts by telephone or email in the event of a disaster or other

contingency that disrupts the normal operation of one or both of the connected systems.

- **Material Changes to System Configuration**: Planned technical changes to the system architecture will be reported to technical staff before such changes are implemented. The initiating organization agrees to conduct a risk assessment based on the new system architecture and to modify and re-sign the ISA within one (1) month of implementation.
- **New Interconnections:** The initiating organization will notify the other organization at least one (1) month before it connects its IT system with any other IT system, including systems that are owned and operated by third parties.
- **Personnel Changes:** The organizations agree to provide notification of the separation or long-term absence of their respective system owner or technical lead. In addition, all organizations will provide notification of any changes in point of contact information. All organizations will also provide notification of changes to user profiles, including users who resign or change job responsibilities.

6 INTERCONNECTION SECURITY AGREEMENT

The technical details of the interconnection will be documented in an ISA. The organizations agree to work together to develop the ISA, which must be signed by all agencies before the interconnection is activated. Proposed changes to any interconnected system or the interconnecting medium will be reviewed and evaluated to determine the potential impact on the interconnection. The ISA will be renegotiated before changes are implemented. Signatories to the ISA shall be the designated organization approval authority for each system.

7 SECURITY

All agencies agree to work together to ensure the joint security of the connected systems and the data they store, process, and transmit, as specified in the ISA. Each organization certifies that its respective system is designed, managed, and operated in compliance with all relevant laws, regulations, and policies.

8 COST CONSIDERATIONS

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

All agencies agree to <apportion percentagewise, equally share> the costs of the interconnecting mechanism and/or media. No such expenditures or financial commitments shall be made without the written concurrence of all affected organizations. Modifications to either system that are necessary to support the interconnection are the responsibility of the respective system owners' organization.

9 TIMELINE

This agreement will remain in effect for <one (1) year> after the last date on either signature in the signature block below. After <one (1) year>, this agreement will expire without further action. If the organizations wish to extend this agreement, they may do so by reviewing, updating, and reauthorizing this agreement. The newly signed agreement should explicitly supersede this agreement, which should be referenced by title and date. If one or more of the agencies wish to terminate this agreement prematurely, they may do so upon 30 days' advanced notice or in the event of a security incident that necessitates an immediate response.

10 SIGNATORY AUTHORITY

I agree to the terms of this Memorandum of Understanding (or Agreement).

(Signature)	(Date)	(Signature)	(Date)
<Organization_A Official name>		<Organization_B Official name>	
<Organization_A Official title>		<Organization_B Official title>	

ANNEX C

SYSTEM INTERCONNECTION ARCHITECTURE

Annex C provides guidance for developing a System Interconnection Implementation Plan and is based on the discussion in section 4.

1 INTRODUCTION

In the introduction, the appropriate personnel should describe the purpose and scope of the implementation plan, and identify the policy requirements and/or guidance on which the system interconnection is based. The networks and IT systems that will be interconnected, the organizations that own them, and the purpose for which they are used should also be identified. In addition, the appropriate personnel should discuss the purpose for interconnecting the systems, describe the services that will be offered over the interconnection, and briefly describe each section of the document.

2 SYSTEM INTERCONNECTION DESCRIPTION

2.1 GENERAL

This section of the plan should include a description of the interconnection architecture, including security controls, hardware, software, servers, and applications. A diagram of the interconnection showing all relevant components should also be included.

2.2 SECURITY CONTROLS

This section should include an identification and description of the security controls currently in place for the networks and IT systems that will be interconnected. After identifying threats that could compromise the system interconnection, a description of how existing security controls will be configured to mitigate those threats should be created. New security controls that will be implemented, including network- and application-level controls should be identified.

2.3 SYSTEM HARDWARE

Hardware that is currently used on the systems to be interconnected and new hardware to be installed as part of the interconnection should be identified and described. The description should include the hardware's function as well as how the hardware will support the interconnection.

2.4 SYSTEM SOFTWARE

Software that is currently used on the systems to be interconnected and new software to be installed as part of the interconnection should be identified and described. The description of current software should include how it will support the interconnection, and the description of new software should include its function.

2.5 DATA/INFORMATION EXCHANGE

Organizations connect networks and IT systems to share locally unavailable resources (e.g., ground station antenna), share data, make data available, or to pass data in one direction from one organization to the other. It may be necessary to install a database that is dedicated to the interconnection. The type(s) of data that will be exchanged between the organizations should be identified, and the transmission methods that will be used should be described. How the data will be stored and processed should also be identified, and a data flow diagram should be provided.

2.6 SERVICES AND APPLICATIONS

The services and applications that the participating organizations will provide over the interconnection should be described, as well as any new services or applications that will be developed, both initially and in the future. Examples include SLE, email, database query, file query, general computational services, application servers, and authentication servers.

3 ROLES AND RESPONSIBILITIES

Once the personnel who will establish and maintain the system interconnection have been identified their respective roles and responsibilities must be defined. A variety of staff skills may be required, including a program manager, network architect, security specialist, system administrator, network administrator, database administrator, application developer, and graphics designer. Staff from all interconnected organizations should be involved, if appropriate. The responsibilities of staff that will be authorized to use the interconnection after it is established (i.e., the users) should be identified as well. The interconnection rules of behavior should be consulted when developing this section.

4 TASKS AND PROCEDURES

4.1 GENERAL

In this section, a step-by-step approach to establishing the interconnection, based on a series of tasks and procedures, should be provided. A list of suggested tasks is provided below. Organizations should view them in the context of their own requirements. A checklist should be provided for each task to ensure it is performed properly.

4.2 IMPLEMENT SECURITY CONTROLS

The process of interconnecting networks and IT systems could open an organization to a range of security vulnerabilities. Consequently, the first step that agencies should take is to implement appropriate security controls. Procedures should be provided for configuring current controls and, if necessary, implementing new controls. Security controls may include firewalls, identification and authentication mechanisms, logical access controls, encryption devices, IDSes, and physical security measures.

4.3 INSTALL HARDWARE AND SOFTWARE

If required, procedures should be provided for configuring or installing the hardware and software needed to establish the interconnection.

4.5 INTEGRATE APPLICATIONS

If required, procedures for linking applications across the interconnection and for providing procedures for developing and implementing new applications should be provided.

4.6 CONDUCT A RISK ASSESSMENT9

In this section, the process for conducting an assessment to identify risks associated with the newly established interconnection should be described. Otherwise, this section should refer to an organization's existing risk assessment methodology. How risks will be addressed should be discussed. For example, risks may be mitigated by adjusting security controls or by implementing additional countermeasures.

4.7 CONDUCT OPERATIONAL AND SECURITY TESTING

Detailed test procedures verifying whether the interconnection operates efficiently and securely should be provided. A description of how the results of the testing will be measured, and how deficiencies will be addressed should be included as well.

4.8 CONDUCT SECURITY TRAINING AND AWARENESS

This section should include a description of a training and awareness program for all personnel who will be authorized to manage, use, and/or operate the system interconnection, including any new computer applications associated with it. Training should ensure that authorized personnel know the rules of behavior associated with the interconnection and how to request assistance if they encounter problems. In addition, personnel who are responsible for

[9] Alternatively, each organization may decide to recertify and reaccredit its respective system, as discussed in 4.2.7.

maintaining the interconnection should receive specialized training to ensure they are proficient in their responsibilities.

5 SCHEDULE AND BUDGET

A schedule for establishing the interconnection, including the estimated time required to complete each task, should be included in this section. A budget, including a description of how the costs will be apportioned between the participating agencies, should also be defined if required.

6 DOCUMENTATION

This section should cite or include all documentation relevant for establishing the interconnection, including system security plans, design specifications, and standard operating procedures.