CCSDS Historical Document

This document's Historical status indicates that it is no longer current. It has either been replaced by a newer issue or withdrawn because it was deemed obsolete. Current CCSDS publications are maintained at the following location:

http://public.ccsds.org/publications/

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-1

GREEN BOOK

November 2007

CCSDS HISTORICAL DOCUMENT

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-1

GREEN BOOK
November 2007

AUTHORITY

Issue:	Informational Report, Issue 1
Date:	November 2007
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 the *Procedures Manual for the Consultative Committee for Space Data Systems*.

This document is published and maintained by:

CCSDS Secretariat
Space Communications and Navigation Office, 7L70
Space Operations Mission Directorate
NASA Headquarters
Washington, DC 20546-0001, USA

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 the *Procedures Manual for the Consultative Committee for Space Data Systems*. 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 addressed to the CCSDS Secretariat at the 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.
- British National Space Centre (BNSC)/United Kingdom.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (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.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- Centro Tecnico Aeroespacial (CTA)/Brazil.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Korea Aerospace Research Institute (KARI)/Korea.
- MIKOMTEK: CSIR (CSIR)/Republic of South Africa.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Organization (NSPO)/Taiwan.
- Naval Center for Space Technology (NCST)/USA.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- 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

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]) which was produced in August 2002.

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

Many space agencies using CCSDS recommendations 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 agencies 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 agency networks and IT systems for other purposes as determined to be required by the agencies themselves.

1.3 APPLICABILITY

1.3.1 APPLICABILITY OF THIS RECOMMENDATION

This recommendation is applicable to all space agencies 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 space agencies have already interconnected networks and IT systems using 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 those space agencies 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. Space agencies 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 that 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 space agencies 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 space agencies develop and execute a plan for establishing the interconnection including implementing, configuring, and testing appropriate security controls.
- **Maintaining the interconnection:** the space agencies 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 space agencies may choose to terminate the interconnection. The termination should be conducted in a planned manner to avoid disrupting the other agency's systems. In response to an emergency, however, one or all space agencies 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.

The 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 space agencies. Finally, the 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 guide for developing an Interconnection Security Agreement, which documents the technical requirements of the interconnection, as well as a sample agreement. Annex B provides a guide for developing a Memorandum of Understanding/Agreement, which defines the responsibilities of the participating space agencies, as well as a sample memorandum. 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.

Access Control: The process of granting access to information technology (IT) system resources only to authorized users, programs, processes, or other systems.

Audit Trail: A record showing who has accessed an IT system and what operations the user has performed during a given period.

Authenticate: To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. Also, to verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

Authentication: The process of verifying the authorization of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

Certification and Accreditation (C&A): The testing and evaluation of the technical and non-technical security features of an IT system to determine its compliance with a set of specified security requirements. Accreditation is a process whereby an authorizing management official authorizes an IT system to operate for a specific purpose using a defined set of safeguards at an acceptable level of risk.

Common Criteria (CC): International standard for computer security (see references [2]-[4]). The Common Criteria does not provide a list of security requirements or features that products must contain. Instead, it describes a framework in which computer system users can specify their security requirements, developers can make claims about the security attributes of their products and evaluators can determine if products actually meet their claims. The Common Criteria provides assurance that the process of specifying, developing, and evaluating a computer security product has been conducted in a rigorous manner.

Data Element: A basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location.

Dedicated Line: A leased or privately owned transmission line that provides a constant transmission path from point A to point B.

Disconnection: The termination of an interconnection between two or more IT systems. A disconnection may be planned (e.g., due to changed business needs) or unplanned (i.e., due to an attack or other contingency).

E1 Line: A telecommunications line with bandwidth capacity of 2.048 Mb/s full-duplex.

E3 Line: A telecommunications line with bandwidth capacity of 34.368 Mb/s full-duplex.

Encryption: The translation of data into a form that is unintelligible without a deciphering mechanism.

File Transfer Protocol (FTP): An Internet standard protocol (reference [5]) that supports file transfer between computers.

Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

Hub: A common connection point for devices in a network. Hubs commonly are used to pass data from one device (or segment) to another.

Identification: The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

Integrated Services Digital Network (ISDN): A public-switched network providing digital connections for the concurrent transmission of voice, video, data, and images.

Interconnection Security Agreement (ISA): In this guide, an agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.

Intrusion Detection System (IDS): A software application that can be implemented on host operating systems or as network devices to monitor activity that is associated with intrusions or insider misuse, or both.

Java: A programming language developed by Sun Microsystems. Java contains a number of features that make it well suited for use on the World Wide Web.

JavaScript: A scripting language for use in developing interactive Web sites.

Kerberos: An authentication system developed at the Massachusetts Institute of Technology (MIT). Kerberos makes use of a trusted third party to enable two parties to exchange private information across a public network (see reference [6]).

Memorandum of Understanding/Agreement (MOU/A): A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.

RADIUS (Remote Authentication Dial-In User Service): An authentication and accounting system used to control access to systems and networks (reference [7]).

Risk: The net mission impact considering the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and the resulting impact if this should occur.

Router: On a network, a device that determines the best path for forwarding a data packet toward its destination.

Security Controls: Protective measures used to meet the security requirements specified for IT resources.

Server: A computer or device on a network that offers one or more network services. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries).

Space Link Extension (SLE): A Consultative Committee for Space Data Systems (CCSDS) recommendation for the tunneling of data from a spacecraft to a control center over a network (reference [8]).

Switch: A network device that filters and forwards packets between LAN segments.

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

T1 Line: A telecommunications line with bandwidth capacity of 1.54 Mb/s.

T3 Line: A telecommunications line with bandwidth capacity of 45 Mb/s.

Threat: The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Trojan Horse: A computer program containing an apparent or actual useful function that also contains additional functions that permit the unauthorized collection, falsification, or destruction of data.

Virtual Private Network (VPN): A data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them.

Virus: A self propagating malicious computer program segment that attaches itself to an application program or other executable component and leaves no obvious sign of its presence.

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Worm: A computer program or algorithm that replicates itself over a computer network and usually performs malicious actions.

1.7 REFERENCES

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

[1] *Security Guide for Interconnecting Information Technology Systems*. National Institute of Standards and Technology Special Publication 800-47. Gaithersburg, Maryland: NIST, August 2002. <http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf>

[2] *Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 1: Introduction and General Model*. International Standard, ISO/IEC 15408-1:2005. 2nd ed. Geneva: ISO, 2005.

[3] *Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 2: Security Functional Requirements*. International Standard, ISO/IEC 15408-2:2005. 2nd ed. Geneva: ISO, 2005.

[4] *Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 3: Security Assurance Requirements*. International Standard, ISO/IEC 15408-3:2005. 2nd ed. Geneva: ISO, 2005.

[5] *File Transfer Protocol*. STD 9. Reston, Virginia: ISOC, October 1985.

[6] "Kerberos: The Network Authentication Protocol." Massachusetts Institute of Technology. <http://web.mit.edu/Kerberos/>

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

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

NOTE – Refer to appendix E of reference [1] for 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. Space agencies can realize significant benefits through a system interconnection 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 space agencies 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, space agencies 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 space agencies. However nothing in this document precludes the systems or networks from being owned by different parts of the same space agency.

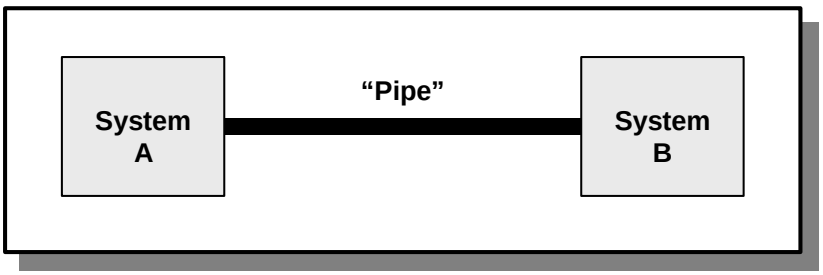

Figure 2-1: Interconnection Components

Space agencies 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, a space agency 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 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 agency may access data and information resources is dependent on its mission and security needs. Accordingly, some space agencies 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 space agencies to added risk. If the interconnection is not properly designed, security failures could compromise the connected systems and the data that 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 agency's system.

It is critical, therefore, that all participating space agencies 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 also is critical that they establish an agreement between themselves regarding the management, operation, and use of the interconnection and that they formally document this agreement. The agreement should be reviewed and approved by appropriate senior staff from each space agency.

[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

The process of connecting networks or IT systems should begin with a planning phase, in which the participating space agencies 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.

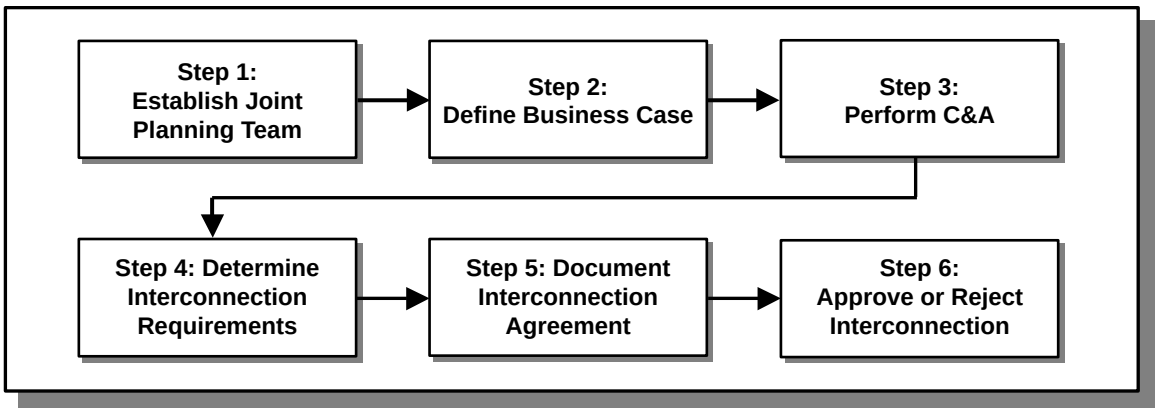

Figure 3-1: Steps to Plan a System Interconnection

3.1 STEP 1: ESTABLISH A JOINT PLANNING TEAM

Each space agency 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 communications between the space agencies 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 agency's network. By coordinating the planning of the interconnection with related activities, the agencies can reduce redundancy and promote efficiency.

3.2 STEP 2: DEFINE THE BUSINESS CASE

The interconnecting space agencies 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 space agencies 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 space agency should consult with its privacy officer or legal counsel to determine whether such information may be shared or transferred. Permission to exchange or transfer data should be documented, along with a commitment to protect such data.

3.3 STEP 3: PERFORM CERTIFICATION AND ACCREDITATION

Before interconnecting, each space agency 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 agency 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) should be used as a mutual C&A process among the interconnecting space agencies. An international standard, the CEM is the common evaluation methodology agreed to by a consortium of twenty-four nations that have agreed mutually to recognize each other's security evaluations.

3.4 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 also may 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 space agencies 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 space agencies 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 space agency and the applications associated with those services. Examples include SLE, e-mail, FTP, RADIUS, Kerberos, database query, file query, and general computational services.

– *Security Controls*. Identify security controls that will be implemented to protect the confidentiality, integrity, and availability of the 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. 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 space agency 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 space agencies 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 space agencies 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 space agencies are compatible, or whether new databases must be normalized so the agencies can use data passed over the interconnection. In addition, determine whether ownership of data is transferred from the transmitting agency to the receiving agency, or whether the transmitting agency retains ownership and the receiver becomes the custodian. As part of this effort, determine how transferred data will be stored, whether data may be re-used, 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 agencies. 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 agencies. 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 space agencies.

- *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 space agencies.

3.5 STEP 5: DOCUMENT INTERCONNECTION AGREEMENT

The joint planning team should document an agreement governing the interconnection and the terms under which the space agencies will abide by the agreement, based on the team's review of all relevant technical, security, and administrative issues (see 3.4, 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.

3.6 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 space agency, 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 space agency 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 space agencies may decide to use already established organizational 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.

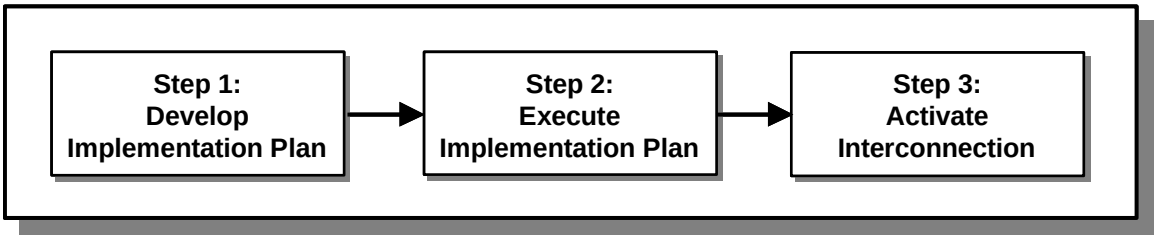

Figure 4-1: Steps to Establish a System Interconnection

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 that 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, by looking for patterns of activity that are associated with intrusions or insider misuse, or both. A combination of network-based and host-based IDSs 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. Space agencies may elect to deploy IPSs in addition to, or in replacement of IDSs.

- *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 space agencies.

- *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 un-encrypted 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, space agencies 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. Use Access Control Lists (ACLs) and access rules to specify the access privileges of authorized personnel, including the level of access and the types of transactions and functions that are permitted (e.g., read, write, execute, delete, create, and search. Configure access rules to grant appropriate access privileges to authorized personnel, based on their roles or job functions. Ensure only system administrators have access to the controls.

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

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

– *Physical and Environmental Security*. Place hardware and software supporting the interconnection, including interconnection points, in a secure location that is protected from unauthorized access, interference, and damage. Ensure that environmental controls are in place to protect against hazards such as fire, water, and excessive heat and humidity. In addition, place computer workstations in secure areas to protect them from damage, loss, theft, or unauthorized physical access. Consider using access badges, cipher locks, or biometric devices to control access to secure areas. Also, consider using biometric devices 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. Place hardware and software in secure areas that are configured with proper environmental controls.

4.2.3 SUBSTEP 3: INTEGRATE APPLICATIONS

Integrate applications or protocols for services that are provided across the interconnection. Examples include SLE, database applications, e-mail, Web browsers, application servers, authentication servers, domain servers, development tools, editing programs, and communications programs. If using Web-based applications, consider the possible security ramifications regarding the use of Java, JavaScript, ActiveX, and cookies.

4.2.4 SUBSTEP 4: CONDUCT OPERATIONAL AND SECURITY TESTING

Conduct and document a series of tests to ensure equipment operates properly and there are no obvious ways for unauthorized users to circumvent or defeat security controls.[7] Test the interface between applications across the interconnection, and simulate data traffic at planned activity levels to verify correct translation at the receiving end(s). Test security controls under realistic conditions. If possible, conduct testing in an isolated, non-operational environment to avoid affecting other systems.

4.2.5 SUBSTEP 5: CONDUCT SECURITY TRAINING AND AWARENESS

Conduct security training and awareness for all authorized personnel who will be involved in managing, using, and/or operating the interconnection. Provide training and awareness for new users and refresher training for all users periodically.

4.2.6 SUBSTEP 6: UPDATE SYSTEM SECURITY PLANS

The space agencies 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, consider conducting mutual reviews of those sections of the updated plans that are relevant to the interconnection. The details for conducting a mutual review should be addressed in the MOU/A.

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

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

- names of interconnected systems;
- space agency 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 space agency 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 3.3. Use of the Common Criteria's Common Evaluation Methodology (CEM) is recommended as a standard evaluation baseline for all space agencies.

4.3 STEP 3: ACTIVATE THE INTERCONNECTION

Activate the interconnection for use by all involved space agencies following prescribed guidelines. It is recommended that one or more of the space agencies test, exercise, and closely monitor the interconnection for a period of at least three months to ensure that it operates properly and securely before going operational. Analyze audit logs carefully and frequently, and monitor the types of assistance requested by users. 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 that 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 space agencies maintain clear lines of communication and communicate regularly to ensure that the interconnection is properly maintained and that security controls remain effective. Open communications also facilitate change management activities by making it easy for all agencies to notify each other about planned system changes that could affect the interconnection. Finally, maintaining clear lines of communication enables all agencies 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 space agencies 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. Space agencies 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 agency 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 space agencies 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 space agencies also be conducted. This testing must be coordinated so that the other agencies 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 agencies, or by an independent third party. All participating space agencies 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 space agencies 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 periodically review the logs to detect patterns of suspicious activity that scanning tools might not recognize. Audit logs should be retained for a period approved by all participating agencies.

5.6 REPORT AND RESPOND TO SECURITY INCIDENTS

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

5.8 PERFORM CHANGE MANAGEMENT

Each space agency should establish a Change Control Board (CCB) to review and approve planned changes to its respective system, such as upgrading software or adding services.

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 space agencies should be notified in writing of the changes, and they should be involved in this process.

If a planned change is designed specifically for the interconnection, the space agencies should establish a joint CCB or a similar body to review and approve the change. In most cases, such changes are designed to improve the operation and security of the interconnection, such as by adding new functions, improving user interfaces, and eliminating (or mitigating) known vulnerabilities.

5.9 MAINTAIN SYSTEM SECURITY PLANS

The space agencies should update their system security plans and other relevant documentation at least annually or whenever there is a significant change to their IT systems or to 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 space agency 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 space agency should notify the other space agencies 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 space agencies 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 appropriate technical staff and approval by senior management.[8]

The system owner or designee should immediately notify the other space agencies' 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 agency 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 space agency 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 space agencies 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 appropriate countermeasures to prevent a recurrence of the problem. They also should modify the ISA and MOU/A to address issues requiring attention, if necessary. Alternatively, if the interconnection has been terminated for more than 90 days, each agency should perform a risk assessment on its respective system and reexamine all relevant planning and implementation issues, including developing a new ISA and MOU/A.

ANNEX A

INTERCONNECTION SECURITY AGREEMENT

The space agencies that own and operate the connected information technology (IT) systems should develop an ISA (or an equivalent document) to document the technical requirements of the interconnection. The ISA also supports an MOU/A between the space agencies (see annex B). An ISA development guide is provided below; a sample ISA is depicted at the end of this annex.

A1 PURPOSE

The intent of the ISA is to document and formalize the interconnection arrangements between "Space Agency A" and "Space Agency B" and to specify any details that may be required to provide overall security safeguards for the systems being interconnected. General guidance regarding the contents of an ISA is provided below; however, an ISA may be tailored by mutual consent of the participating space agencies. A system that is approved by an ISA for interconnection with one agency's system should meet the protection requirements equal to, or greater than those implemented by the other agency's system.

A2 SCOPE

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

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

A3 PROCEDURE

An ISA is used to support an MOU/A that establishes the requirements for data exchange between two space agencies. The MOU/A is used to document the business and legal requirements necessary to support the business relations between the two agencies. The MOU/A should not include technical details regarding how the interconnection is established; that is the function of the ISA. An ISA is a distinct, security-related document that outlines the technical solution and security requirements for the interconnection. It does not replace an MOU/A. As older MOU/As are updated, they should be changed to refer to the appropriate ISA covering the connectivity addressed by the MOU/A.

An ISA can be signed by the space agency authorizing management officials whose names appear in Section 4 of the agreement (see example below). *The ISA should be formally signed before the interconnection is declared operational*.

A4 CONTENTS OF AN INTERCONNECTION SECURITY AGREEMENT

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

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

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

A5 SECTION 1: INTERCONNECTION STATEMENT OF REQUIREMENTS

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

- the requirement for the interconnection, including the benefits derived;
- the names of the systems being interconnected;
- the agency name that initiated the requirement.

A6 SECTION 2: SYSTEM SECURITY CONSIDERATIONS

Use Section 2 to document the security features that are in place to protect the confidentiality, integrity, and availability of the data and the systems being interconnected. All space agencies should answer each item, even if only one agency is affected by the item in question. Note that some items are recommended, whereas others are optional. Optional items affecting only one system should be answered and included.

Suggested items that should appear include:

- *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.
- *Services Offered*. Describe the nature of the information services (e.g., SLE, e-mail, FTP, database query, file query, general computational services) offered over the interconnection by each space agency.
- *Data Sensitivity*. Enter the sensitivity level of the information that will be handled through the interconnection, including the highest level of sensitivity involved (e.g., privacy-related, healthcare-related, trade secrets, mission confidential, sensitive-but-unclassified) and the most restrictive protection measures required.
- *User Community*. Describe the "user community" that will be served by the interconnection, including their approved access levels and the lowest approval level of any individual who will have access to the interconnection. Also, discuss requirements for background investigations and security clearances, if appropriate.
- *Information Exchange Security*. Describe all system security technical services pertinent to the secure exchange of data between the connected systems.
- *Rules of Behavior*. Summarize the aspects of behavior expected from users who will have access to the interconnection. Each system is expected to protect information belonging to the other through the implementation of security controls that protect against intrusion, tampering, and viruses, among others. Do not enter statements of law or policy. Such statements typically are addressed in the MOU/A.
- *Formal Security Policy*. Enter the titles of the formal security policies that govern each system (e.g., "Information Systems Policy and Procedures, Number xxxx" for "Space Agency A").
- *Incident Reporting*. Describe the agreements made regarding the reporting of and response to information security incidents for the space agencies.
- *Audit Trail Responsibilities*. Describe how the audit trail responsibility will be shared by the space agencies and what events each agency will log. Specify the length of time that audit logs will be retained.

Other items that might appear in the ISA include:[9]

- *Security Parameters*. Specify the security parameters exchanged between systems to authenticate that the requesting system is the legitimate system and that the class(es) of service requested is approved by the ISA. For example, at the system level, if a new service such as e-mail is requested without prior coordination, it should be detected, refused, and documented as a possible intrusion until the interconnected service is authorized. Also, additional security parameters may be required (e.g., personal accountability) to allow the respondent system to determine whether a requestor is authorized to receive the information and/or services requested and whether all details of the transaction fall within the scope of user services authorized in the ISA.

- *Operational Security Mode*. If the space agencies use the concept of "Protection Levels" and "Levels-of-Concern" for Confidentiality, Integrity, and Availability based on their implementation of the *Common Criteria*, enter the values for each as documented for both systems. Optionally, the security mode of operations could be documented for both systems.

- *Training and Awareness*. Enter the details of any new or additional security training and awareness requirements, and the assignment of responsibility for conducting training and awareness throughout the life cycle of the interconnection.

- *Specific Equipment Restrictions*. Describe any revised or new restriction(s) to be placed on computer workstations (e.g., PCs, terminals), including their usage, location, and physical accessibility.

- *Dialup and Broadband Connectivity*. Describe any special considerations for dialup and broadband connections to any system in the proposed interconnection, including security risks and safeguards used to mitigate those risks.

- *Security Documentation*. Enter the title and general details of each agency's system security plan, including the assignment of responsibilities for developing and accepting the plan, as well as any other relevant documentation.

[9] The space agencies may choose to address other relevant items in the ISA, in addition to the suggested items. If the technical representatives determine that any item is "not applicable," a statement to that effect may be made in the ISA in lieu of eliminating the item from the ISA.

A7 SECTION 3: TOPOLOGICAL DRAWING

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:

- the title "SECTION 3: TOPOLOGICAL DRAWING";
- all communications links, paths, circuits, and other components used for the interconnection, from "Space Agency A's" system(s) to "Space Agency B's" system(s);
- the logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations).

A8 SECTION 4: SIGNATORY AUTHORITY

The ISA should include a signature line. Optionally, this section may include any statements that the space agency authorizing officials desire in order to finalize the ISA. This section should include the following:

- the expiration date of the agreement;
- periodic review requirements, such as the date of the next review;
- other statements as required by the authorizing officials, if any;
- the signatures of the authorizing officials from each space agency, and the date of the signatures.

[DOCUMENT HANDLING CAVEATS HERE]

INTERCONNECTION SECURITY AGREEMENT

Between "Space Agency A"

and

"Space Agency B"

(ORGANIZATIONAL SEAL[S] HERE)

(DATE HERE)

(Space Agency A)
(Space Agency B)

[DOCUMENT HANDLING CAVEATS HERE]

[DOCUMENT HANDLING CAVEATS HERE]

INTERCONNECTION SECURITY AGREEMENT

SECTION 1: INTERCONNECTION STATEMENT OF REQUIREMENTS

The requirements for interconnection between "Space Agency A" and "Space Agency B" are for the express purpose of exchanging data between "System A," owned by Space Agency A, and "System B," owned by Space Agency B. Space Agency B requires the use of Space Agency A's "XYZ database" and Space Agency A requires the use of Space Agency B's "ABC database," as approved and directed by the Directors of "Space Agency A" and "Space Agency B" in "Proclamation Z," dated (date). The expected benefit is to expedite the processing of data associated with "Project R" within prescribed timelines.

SECTION 2: SYSTEM SECURITY CONSIDERATIONS

- **General Information/Data Description.** The interconnection between System A, owned by Space Agency A, and System B, owned by Space Agency B, is a two-way path. The purpose of the interconnection is to deliver the XYZ database to Space Agency B's Data Analysis Department and to deliver the ABC database to Space Agency A's Research Office.
- **Services Offered.** No user services are offered. This connection only exchanges data between Space Agency A's system and Space Agency B's system via a dedicated in-house connection.
- **Data Sensitivity.** The sensitivity of data exchanged between Space Agency A and Space Agency B is unclassified and proprietary.
- **User Community.** All Space Agency A users with access to the data received from Space Agency B are citizens of Space Agency A's country with a valid and current Space Agency A background investigation. All Space Agency B users with access to the data received from Space Agency A are citizens of Space Agency B's country with a valid and current Space Agency B background investigation.
- **Information Exchange Security.** The security of the information being passed on this two-way connection is protected through the use of approved encryption mechanisms. The connections at each end are located within controlled access facilities, guarded 24 hours a day. Individual users will not have access to the data except through their systems security software inherent to the operating system. All access is controlled by authentication methods to validate the approved users.

[DOCUMENT HANDLING CAVEATS HERE]

1

[DOCUMENT HANDLING CAVEATS HERE]

- **Trusted Behavior Expectations.** Space Agency A's system and users are expected to protect Space Agency B's ABC database, and Space Agency B's system and users are expected to protect Space Agency A's XYZ database, in accordance with mutually agreed upon policies.
- **Formal Security Policy.** Policy documents that govern the protection of the data are Space Agency A's "XXX Policy" and Space Agency B's "YYY Policy."
- **Incident Reporting.** The agency discovering a security incident will report it in accordance with its incident reporting procedures. In the case of Space Agency B, any security incident will be reported to the Computer Security Incident Response Capability located at the Data Security Complex. Policy governing the reporting of Security Incidents is CC-2234.
- **Audit Trail Responsibilities.** Both agencies are responsible for auditing application processes and user activities involving the interconnection. Activities that will be recorded include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs will be retained for one (1) year.

SECTION 3: TOPOLOGICAL DRAWING

(Insert a drawing here.)

SECTION 4: SIGNATORY AUTHORITY

This ISA is valid for one (1) year after the last date on either signature below. At that time it will be updated, reviewed, and reauthorized. Either agency may terminate this agreement upon 30 days' advanced notice in writing or in the event of a security incident that necessitates an immediate response.

(Space Agency A Official)	**(Space Agency B Official)**
----------	**----------**
(Signature Date)	(Signature Date)

[DOCUMENT HANDLING CAVEATS HERE]

2

ANNEX B

MEMORANDUM OF UNDERSTANDING/AGREEMENT

The space agencies that own and operate the connected systems should establish an MOU/A (or an equivalent document) that defines the responsibilities of all agencies 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 space agencies may use their own MOU/A format, if appropriate. A sample MOU/A is attached at the end of this annex.

B1 SUPERSESSION

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

B2 INTRODUCTION

Describe the purpose of the memorandum. Sample language is provided in the sample memorandum. Identify the space agencies, networks, and IT systems that are involved in the interconnection.

B3 AUTHORITIES

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

B4 BACKGROUND

Describe 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.

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

B5 COMMUNICATIONS

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

B6 INTERCONNECTING SECURITY AGREEMENT

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

B7 SECURITY

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

B8 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 space agency is responsible for the equipment necessary to interconnect its local system, whereas the agencies jointly fund the interconnecting mechanism or media.

B9 TIMELINE

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

B10 SIGNATORY AUTHORITY

The memorandum must include a signature line, containing signature blocks for each space agency designated approval authority.

[DOCUMENT HANDLING CAVEATS HERE]

MEMORANDUM OF UNDERSTANDING (OR AGREEMENT)

Between

“Space Agency A”

and

“Space Agency B”

(ORGANIZATIONAL SEAL[S] HERE)

(DATE HERE)

(Space Agency A) **(Space Agency B)**

[DOCUMENT HANDLING CAVEATS HERE]

[DOCUMENT HANDLING CAVEATS HERE]

MEMORANDUM OF UNDERSTANDING (OR AGREEMENT)

SUPERSEDES: (None or document title and date)

INTRODUCTION

The purpose of this memorandum is to establish a management agreement between "Space Agency A" and "Space Agency B" regarding the development, management, operation, and security of a connection between "System A," owned by Space Agency A, and "System B," owned by Space Agency B. This agreement will govern the relationship between Space Agency A and Space Agency B, including designated managerial and technical staff, in the absence of a common management authority.

AUTHORITY

The authority for this agreement is based on "Proclamation A" issued by the Directors of "Space Agency A" and "Space Agency B" on (date).

BACKGROUND

It is the intent of both space agencies to this agreement to interconnect the following information technology (IT) systems to exchange data between "ABC database" and "XYZ database." Space Agency A requires the use of Space Agency B's ABC database, and Space Agency B requires the use of Space Agency A's XYZ database, as approved and directed by the Secretary of Agency in Proclamation A. The expected benefit of the interconnection is to expedite the processing of data associated with "Project R" within prescribed timelines.

Each IT system is described below:

- **SYSTEM A**
  - Name
  - Function
  - Location
  - Description of data, including sensitivity
- **SYSTEM B**
  - Name
  - Function
  - Location
  - Description of data, including sensitivity

[DOCUMENT HANDLING CAVEATS HERE]

1

[DOCUMENT HANDLING CAVEATS HERE]

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 System A and System B agree to designate and provide contact information for technical leads for their respective system, and to facilitate direct contacts between technical leads to support the management and operation of the interconnection. To safeguard the confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit, the 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 e-mail when a security incident(s) is detected, so the other agency may take steps to determine whether its system has been compromised and to take appropriate security precautions. The system owner will receive formal notification in writing within five (5) business days after detection of the incident(s).
- **Disasters and Other Contingencies:** Technical staff will immediately notify their designated counterparts by telephone or e-mail in the event of a disaster or other contingency that disrupts the normal operation of one or both of the connected systems.
- **Material Changes to System Configuration:** Planned technical changes to the system architecture will be reported to technical staff before such changes are implemented. The initiating space agency 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 space agency will notify the other space agency 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 space agencies agree to provide notification of the separation or long-term absence of their respective system owner or technical lead. In addition, all agencies will provide notification of any changes in point of contact information. All agencies also will provide notification of changes to user profiles, including users who resign or change job responsibilities.

[DOCUMENT HANDLING CAVEATS HERE]

2

[DOCUMENT HANDLING CAVEATS HERE]

INTERCONNECTION SECURITY AGREEMENT

The technical details of the interconnection will be documented in an Interconnection Security Agreement (ISA). The space agencies 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 space agency approval authority for each system.

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 agency certifies that its respective system is designed, managed, and operated in compliance with all relevant laws, regulations, and policies.

COST CONSIDERATIONS

All agencies agree to equally share the costs of the interconnecting mechanism and/or media, but no such expenditures or financial commitments shall be made without the written concurrence of all affected space agencies. Modifications to either system that are necessary to support the interconnection are the responsibility of the respective system owners' agency.

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 space agencies 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.

SIGNATORY AUTHORITY

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

(Space Agency A Official)	**(Space Agency B Official)**
----------	**----------**
(Signature Date)	(Signature Date)

[DOCUMENT HANDLING CAVEATS HERE]

3

ANNEX C

SYSTEM INTERCONNECTION IMPLEMENTATION PLAN

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

C1 INTRODUCTION

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

C2 SYSTEM INTERCONNECTION DESCRIPTION

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

C2.1 SECURITY CONTROLS

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

C2.2 SYSTEM HARDWARE

Identify and describe the hardware that is currently used on the systems that will be interconnected, and describe how it will support the interconnection. Identify and describe any new hardware that will be installed as part of the interconnection, including its function.

C2.3 SYSTEM SOFTWARE

Identify and describe software currently used on the systems that will be interconnected, and describe how it will be used to support the interconnection. Identify any new software that will be installed as part of the interconnection, including its function.

C2.4 DATA/INFORMATION EXCHANGE

Space agencies connect networks and IT systems to share locally unavailable resources (e.g., ground station antenna), share data, make data available, or pass data one-way from one agency to the other. It may be necessary to install a database that is dedicated to the interconnection. Identify the type(s) of data that will be exchanged between the space agencies, and describe the transmission methods that will be used. Identify how the data will be stored and processed. Provide a data flow diagram.

C2.5 SERVICES AND APPLICATIONS

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

C3 ROLES AND RESPONSIBILITIES

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

C4 TASKS AND PROCEDURES

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

C4.1 IMPLEMENT SECURITY CONTROLS

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

C4.2 INSTALL HARDWARE AND SOFTWARE

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

C4.3 INTEGRATE APPLICATIONS

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

C4.4 CONDUCT A RISK ASSESSMENT[10]

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

C4.5 CONDUCT OPERATIONAL AND SECURITY TESTING

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

C4.6 CONDUCT SECURITY TRAINING AND AWARENESS

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

C5 SCHEDULE AND BUDGET

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

C6 DOCUMENTATION

Cite or include all documentation that is relevant for establishing the interconnection, including system security plans, design specifications, and standard operating procedures.

[10] Alternatively, each space agency may decide to recertify and reaccredit its respective system, as discussed in 4.2.7.