

Report Concerning Space Data System Standards

|  |
| --- |
| Security Guide for Mission Planners |

Draft Informational Report

CCSDS 350.7-G-1

Draft Green Book

November 2010

AUTHORITY

|  |
| --- |
|  |
|  | Issue: | Draft Green Book, Issue 1 |  |
|  | Date: | November 2010 |  |
|  | Location: | Not Applicable |  |
|  |

**(WHEN THIS INFORMATIONAL REPORT IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF AUTHORITY:)**

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

[Foreword text specific to this document goes here. The text below is boilerplate.]

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.
* China National Space Administration (CNSA)/People’s Republic of China.
* 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)/Chinese Taipei.
* 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 and Issue** | **Date** | **Status** |
| CCSDS 350.7-G-1 | Security Guide for Mission Planners, Draft Informational Report, Issue 1 | November 2010 | Original issue |
|  |  |  |  |
|  |  |  |  |

CONTENTS

Section Page

[DOCUMENT CONTROL iv](#_Toc276453618)

[CONTENTS v](#_Toc276453619)

[1 Introduction 1-1](#_Toc276453620)

[1.1 PURPOSE 1-1](#_Toc276453621)

[1.2 SCOPE 1-1](#_Toc276453622)

[1.3 APPLICABILITY 1-1](#_Toc276453623)

[1.4 RATIONALE 1-1](#_Toc276453624)

[1.5 Document Structure 1-1](#_Toc276453625)

[1.6 Definitions 1-2](#_Toc276453626)

[1.7 References 1-4](#_Toc276453627)

[2 Overview 2-6](#_Toc276453628)

[2.1 Target Audience 2-6](#_Toc276453629)

[2.2 Security Concepts 2-6](#_Toc276453630)

[2.3 Security Management 2-6](#_Toc276453631)

[3 Security Planning 3-7](#_Toc276453632)

[3.1 Security Policy 3-8](#_Toc276453633)

[3.2 INFORMATION CATEGORIZATION 3-9](#_Toc276453634)

[3.3 THREAT ASSESSMENT 3-9](#_Toc276453635)

[3.4 Security REQUIREMENTS & Controls 3-9](#_Toc276453636)

[3.4.1 USE OF STANDARDS 3-10](#_Toc276453637)

[3.5 Security Plan 3-10](#_Toc276453638)

[3.5.1 SYSTEM DEFINITION 3-10](#_Toc276453639)

[3.5.2 RISK ASSESSMENT 3-11](#_Toc276453640)

[3.5.3 APPROVAL AND LIFE CYCLE 3-11](#_Toc276453641)

[4 SECURITY CONTROLS FRAMEWORKS 4-12](#_Toc276453642)

[4.1 ISO/IEC 27000 Series 4-12](#_Toc276453643)

[4.2 OTHER FRAMEWORKS 4-12](#_Toc276453644)

[4.3 SPECIAL CONSIDERATIONS FOR SPACE SYSTEMS 4-12](#_Toc276453645)

# Introduction

## PURPOSE

This Guide is intended to provide guidance to mission planners in developing the management, operational and technical security controls appropriate to the value of their system and the information processed in it.

## SCOPE

THE INFORMATION CONTAINED IN THIS REPORT IS NOT PART OF ANY OF THE CCSDS RECOMMENDED STANDARDS. In the event of any conflict between any CCSDS Recommended Standard and the material presented herein, the CCSDS Recommended Standard shall prevail.

Other CCSDS Recommended Standards and “Green Book” informational reports listed in section 1.7, “References”, provide more detail on particular aspects of assessing risks and implementing technical security measures.

## APPLICABILITY

## RATIONALE

The purpose of this guide is to introduce the reader to best practices in information security, and to provide a structured process flow and templates to help ensure that security aspects pertinent to space systems are not overlooked.

To date, space missions have implemented a wide variety of generally mission-specific protections for space systems and data. Information security best practices have only recently been defined and agreed-to as recognized standards across industries and national boundaries. As space systems become increasingly more interconnected with ground-based I/T networks even including the Internet, it becomes more important to provide an integrated approach to addressing not only the security concerns traditionally understood to space systems designers, but also those more typical of I/T environments.

## Document Structure

This document is organized as follows:

Section 2 provides an introduction to security, defines terms that are used in this report, and identifies generic space mission security threats.

Section 3 describes the security planning process from policy definition through risk assessment and security control selection, to architecture and requirements.

Section 4 presents an introduction to common security controls and describes some controls specific to space data systems.

Annex A provides a sample template for performing security planning that incorporates the ISO 27000 series of security controls, tailored for applicability to the lifecycle and operational environment of many space data systems.

## Definitions

Access Control: The process of granting access to the resources of a system only to authorized users, programs, processes, or other systems.

Access Control Mechanism: Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access in an automated system.

Authentication: (1) Verification of 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. (2) Verification of the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

Authorization: The granting of access rights to a user, program, or process.

Compensating Controls: Any control that is used in a system to compensate for the absence of another control that is prescribed or expected. The use of compensating controls needs to be thoroughly documented and the risks understood.

Common Controls: Security controls that are applied to more than one system through shared organizational procedures or infrastructure.

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Configuration Management: Process of controlling modifications to the system’s hardware, firmware, software, and documentation which provides sufficient assurance the system is protected against the introduction of improper modification before, during, and after system implementation.

Data Integrity: Condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Denial of Service: Any action or series of actions that prevents any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service.

Identification: The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

Masquerading: Attempts to gain access to a system by posing as an authorized user or as a process. This is a form of spoofing.

Residual Risk: The portion of risk that remains after security measures have been applied.

Risk: A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact.

NOTE – Risk is the loss potential that exists as the result of threat and vulnerability pairs. It is a combination of the likelihood of an attack (from a threat source) and the likelihood that a threat occurrence will result in an adverse impact (e.g., denial of service, loss of confidentiality or integrity), and the severity of the resulting adverse impact. Reducing either the threat or the vulnerability reduces the risk.

Risk Analysis: An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. The purpose of a risk assessment is to determine if countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level.

Security Policy: The set of laws, rules, and practices that regulate how information is managed, protected, and distributed.

NOTE – A security policy may be written at many different levels of abstraction. For example, a corporate security policy is the set of laws, rules, and practices within a user organization; system security policy defines the rules and practices within a specific system; and technical security policy regulates the use of hardware, software, and firmware of a system or product.

Threat: Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Threat Agent: A method used to exploit a vulnerability in a system, operation, or facility.

Threat Analysis: The examination of all actions and events that might adversely affect a system or operation.

Threat Assessment: Formal description and evaluation of threat to a system.

Trojan Horse: A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity.

Virus: A program that can ‘infect’ other programs by modifying them to include a, possibly evolved, copy of itself.

Vulnerability: Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to violate system security policy.

Vulnerability Analysis: The systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

Vulnerability Assessment: A measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack.

## 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. *The Application of CCSDS Protocols to Secure Systems*. Informational Report, CCSDS 350.0-G-2. Green Book. Issue 2. Washington, D.C.: CCSDS, January 2006.
2. *Security Architecture for Space Data Systems*. Recommendation for Space Data System Practices, CCSDS 351.0-M-1. Magenta Book. Washington, D.C.: CCSDS, 2010.
3. *Security Threats Against Space Missions*. Informational Report, CCSDS 350.1-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, October 2006.
4. *CCSDS Guide for Secure System Interconnection*. Informational Report, CCSDS 350.4-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, November 2007.
5. *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*. International Standard, ISO/IEC 7498-1. 2nd ed. Geneva: ISO, 1994.
6. *Information Technology—Security Techniques— Information Security Management Systems — Overview and Vocabulary*. International Standard, ISO/IEC 27000:2005. 1st ed. Geneva: ISO, 2005.
7. *Information Technology—Security Techniques— Information Security Management Systems — Requirements*. International Standard, ISO/IEC 27001:2005. 1st ed. Geneva: ISO, 2005.
8. *Information Technology—Security Techniques—Code of Practice for Information Security Management*. International Standard, ISO/IEC 27002:2005. 2nd ed. Geneva: ISO, 2005.
9. *Information Technology—Security Techniques—Information Security Management System Implementation Guidance*. International Standard, ISO/IEC 27003:2010. 1st ed. Geneva: ISO, 2010.
10. *Information Technology—Security Techniques—Information Security Management—Measurement*. International Standard, ISO/IEC 27004:2009. 1st ed. Geneva: ISO, 2009.
11. *Information Technology—Security Techniques—Information Security Risk Management*. International Standard, ISO/IEC 27005:2008. 1st ed. Geneva: ISO, 2008.
12. Idaho State University, Glossary of INFOSEC and INFOSEC Related Terms, SIMPLOT Decision Center, August 1996.

# Overview

## Target Audience

This document is intended to provide the mission planner, program manager, and/or engineering lead with a basic understanding of the strategy, purpose, and process flow of integrating security early into the development of a space system.

## Security Concepts

The objective of system security planning is to improve the protection of information and information system resources in order to assure sustained mission success and continuity. Both space systems information and equipment are subject to a variety of threats (natural, accidental, and deliberate) and require varying degrees of protection depending upon the nature of the mission and the value of physical and informational assets.

## Security Management

Each organization should develop, document, and implement an organization-wide program to provide information security for the information and information systems that support the operations and assets of that organization. ISO/IEC 27000 (reference [6]), which provides a broad overview of information security management, calls this program an “information security management system” (ISMS).

According to ISO/IEC 27000: *“Information security is achieved through the implementation of an applicable set of controls, selected through the chosen risk management process and managed using an ISMS, including policies, processes, procedures, organizational structures, software and hardware to protect the identified information assets. These controls need to be specified, implemented, monitored, reviewed and improved where necessary, to ensure that the specific security and business objectives of the organization are met. Relevant information security controls are expected to be seamlessly integrated with an organization's business processes.”*

# Security Planning

The objective of a security plan is to provide in one place an assessment, updated on an ongoing basis, of the present status of the system's security protections and risks. The security plan is essential to informing management decisions and establishing accountability for the development and maintenance of security protections.

Every mission should have a security plan and a risk assessment. This guide is directed toward the development and use of the mission's security plan.

The security plan should either include or reference applicable system policies, security architecture, and operating procedures. These are discussed in more detail in references [1] and [2] . It should also include or reference a risk assessment that matches the threats to the system with known vulnerabilities that could be used to carry out a threat, and the potential impacts of each to the system, as discussed in reference [3].



Figure ‑. CCSDS Security Document Tree

 depicts the logical organisation of existing CCSDS security-related documentation. Some documents may still be in the review stage. depicts how these documents have evolved from a single “Green Book” to a more fully-developed security framework and core suite of security recommendations to the mission designer. Areas of potential future CCSDS work are tentatively outlined, but unofficial as of this time.



Figure ‑. Evolution of CCSDS Security Framework

## Security Policy

A system's security policy is its “concept of operations” with respect to security. It outlines how the system (which may be either considered broadly as a combination of infrastructure, multiple hardware and software components, and the individuals operating and maintaining them, or considered narrowly as a particular component in isolation) is intended to operate, and what action is to be taken when it operates outside its intended parameters.

Every mission should define a security policy as an element of its overall mission concept definition. The mission security policy must be observant of any higher-level organization security policies but must clearly state:

1. the classification and therefore level of protection of all the information (e.g., telemetry, telecommand, software, and ground systems data) associated with the mission, both live and archive;
2. the roles of those who have access to the system;
3. the integrity requirements of the system; and
4. the availability requirements of the system.

A well-considered security policy should precede system requirements definition, and will help to minimize the risk of unforeseen security problems later in implementation.

## INFORMATION CATEGORIZATION

In order to select appropriate security controls, organizations must clearly understand the criticality and sensitivity of the information that will be handled by the system according to the criteria of confidentiality, availability, and integrity. Many systems will handle several different data types each with different attributes. One example of information criticality and sensitivity categories applicable to various systems may be found in [B6].

Military or dual-use systems are usually subject to national security classification regulations which override organizational discretion in categorizing information. Civil systems may be bound by other laws (e.g., export and copyright restrictions) controlling the handling of specific information types. Organizations should still identify their system’s operational availability and integrity needs for the information, since these needs may be unaddressed by legal and national-security requirements pertaining to information confidentiality.

## THREAT ASSESSMENT

The threat assessment needs to consider the type of the mission and what the information security threats are to that mission. It is important to consider all parts of the mission architecture during all phases of the mission as the threat profile to the mission will change as the mission progresses. For a more detailed discussion of mission threat assessment, see reference [3].

It should be noted that the threat assessment will use the outputs of the Security Policy and Security Interconnection documents to help identify attack vectors and the value of the data and assets to be protected.

## Security REQUIREMENTS & Controls

Organizations must adopt a set of security controls and a process to implement and manage those controls in order to protect their information and information systems. The controls selected or planned must be documented in system requirements documentation.

Security requirements derive from security policy as well as functional system requirements with implications to security. It is important to keep the two concepts separate; while requirements mandate system capabilities, policy mandates the uses of those capabilities. For example, to reject commands that fail authentication is a policy; to build a capability that can authenticate commands is a requirement. Avoid placing security policy statements into requirements documents. Requirements should state the capabilities needed in order to implement the security policy.

Similarly, avoid placing “negative” security requirements into requirements documents, i.e., expressing a requirement that something should *not* occur. Such requirements are difficult to test for compliance. It is commonplace within I/T to encounter systems that pass all functional testing and yet have obvious, easily exploited security flaws. This is usually explainable by functional tests that prove what the system does, and not what it does not do.

Security controls provide the mapping from requirements and policy to system design and operations. Most security controls may be classed as belonging to one of three basic types: *protective*, *detective*, or *reactive*. Protective controls are measures designed to prevent a negative event from occurring, while detective controls aim to inform the organization about an event, and reactive controls are “after the fact” measures to restore the system to nominal operation and/or collect forensic information about the nature and extent of the event.

Organizations must also maintain a mission system’s security controls throughout the lifetime of the mission, as described below in section 3.5.3.

### USE OF STANDARDS

Security must be an integral part of the overall system design. Security flaws are often subtle, and the most troublesome security design flaws arise from unintended effects of interactions between components in a system; such vulnerabilities cannot be easily remedied as can mere programming errors. It is greatly helpful to employ proven and well-known standards in security designs.

This is particularly true in the field of cryptographic mechanisms. Algorithms that have been subjected to peer review by cryptographers are, in general, more mathematically robust and less likely to contain hidden weaknesses.

## Security Plan

Each organization should develop a system security plan that references or provides a summary of the system security requirements, describes the security controls in place or planned for meeting those requirements, and describes the risk assessment of the system. The plan also describes organizational decisions for what is to be done about any discrepancies (including whether to accept risk & proceed as-is).

The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. Additional information may be included in the plan and the format organized according to organizational needs, so long as the major sections described in this document are adequately covered and readily identifiable.

### SYSTEM DEFINITION

A security plan may have multiple subsystems or subordinate systems that inherit their policies and/or controls. The mission planner should include both space and ground elements in defining security for the early stages of planning, although each should have its own security plan as development progresses toward implementation.

A security plan should generally describe resources under the same direct management control. Where a complex system includes interacting elements under different management control (e.g., spacecraft and ground systems), those elements should be described separately and interactions between them should be carefully noted. Additionally, there must be assurance that any shared resources (e.g., organizational processes, networks, and physical facilities), are adequate for the highest criticality and sensitivity handled.

The security plan should follow the functional organization of the system. The process of uniquely assigning information resources to an information system defines the security boundary for that system. The security boundary should take into account regulatory authority, trust relationships, and line management authority.

### RISK ASSESSMENT

The risk assessment uses the output of the threat assessment to assess the likelihood of any potential impact occurring. Risk assessment involves assessing what vulnerabilities exist in the system that also correspond to an identified threat. In the early stages of development, vulnerabilities may be theoretical in nature; in later stages, they will be highly dependent upon implementation details.

Risk is a function of the impact of an occurrence and the likelihood of that impact's occurrence. Impact may be considered qualitatively (e.g., low/medium/high) or quantitatively (e.g., lost revenue due to outages) according to organizational needs.

The risk assessment should also identify, for each risk found, a mitigation strategy (to be prioritized and scheduled as the organization chooses) or a recommendation simply to accept the risk.

### APPROVAL AND LIFE CYCLE

Organizational policy should clearly define who is responsible for approving the system security plan. By authorizing the system to operate, the manager accepts its associated risks.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the system security plan establishes and documents the security controls, risk assessment, and risk mitigation actions or acceptance of residual risks, it should form the basis for the authorization.

The applicability and usefulness of the security controls originally implemented should be periodically re-evaluated as threats to the system change over time, and especially as system components are replaced or upgraded during normal maintenance. Security controls should be changed as appropriate to adapt to changes in their associated threats and specific vulnerabilities in system components. Where applicable, a periodic review of the system security plan should be used to renew the management authorization.

# SECURITY CONTROLS FRAMEWORKS

The purpose of a security controls framework is to provide a hierarchical grouping of related security concerns to guide the system owner in setting policy and aid in decomposing policy into more specific architectural and procedural requirements for implementation. It makes it possible to assess whether and how the system meets its security objectives.

Most frameworks will recommend more stringent or less stringent controls based upon the pre-determined criticality and sensitivity (with respect to confidentiality, availability, and integrity) of the data types the system processes.

## ISO/IEC 27000 Series

The ISO/IEC 27001 standard (reference [7]) identifies a security controls framework encompassing management, operational, and technical capabilities. The framework addresses the most common aspects of protecting the confidentiality, integrity, and availability of information and information systems. There are dozens of individual controls available in the ISO framework, which are organized according to the high-level groupings listed in Table 1 of Annex A. An overview of information security management may be found in ISO/IEC 27000 (reference [6]). The companion ISO/IEC documents numbered 27002-27005 (references [8] - [11]) provide accompanying implementation guidance.

## OTHER FRAMEWORKS

In addition to ISO/IEC standards (and national standards derived from ISO/IEC), there are several widely used security controls frameworks used by private entities and government agencies. Among these are:

1. the National Institute for Standards and Technology (NIST) framework, used by United States civilian government agencies and defined in NIST Special Publications 800-53, 800-60, et al. (references [B5] and [B6]),;
2. the Control Objectives for Information and related Technology (COBIT) (reference [B7]) published by the Informations Systems Audit and Control Association (ISACA);
3. the considerations found in ARINC Report 811 (reference [B8]), “Commercial Aircraft Information Security Concepts of Operation and Process Framework”.

## SPECIAL CONSIDERATIONS FOR SPACE SYSTEMS

In addition to the security controls from a well-known I/T security controls framework such as ISO 27001 are organization- or system-specific security controls that may be locally defined. Some security concerns are particular to space systems and may not be clearly addressed in I/T controls frameworks applicable to generic I/T systems.

The template in Annex A includes some sample controls pertinent to space systems.

1. MISSION SECURITY PLAN TEMPLATE

[The following template is intended to aid the mission planner in understanding and applying recognized best practices in security. It takes the form of a document which would normally be compiled to satisfy organizational directives or a third-party security audit.]

* 1. General System information
		1. System Name

List the system name and/or any unique reference identifier(s) the organization uses.

* + 1. system operational status

Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status:

* Operational
* Under Development
* Major Modification
	+ 1. Responsible individuals
			1. System Owner

This section should identify the individual with overall budgetary and management authority over the development and operation of the system. The person may be identified by title and agency, although it is preferable to include specific individual contact information (e.g., name, e-mail address, and telephone number).

* + - 1. Authorizing Official

This section should identify the individual designated by the organization with overall authority and responsibility to approve the fitness of the system for operation. This may be the system owner or another individual. The person may be identified by title and agency, although it is preferable to include specific individual contact information (e.g., name, e-mail address, and telephone number).

* + - 1. Assignment of Security Responsibility

This section should identify the individual with overall authority and responsibility for the security of the system. The person may be identified by title and agency, although it is preferable to include specific individual contact information (e.g., name, e-mail address, and telephone number).

* + - 1. Other Designated Contacts:

This section should identify other key personnel, if applicable. The person may be identified by title and agency, although it is preferable to include specific individual contact information (e.g., name, e-mail address, and telephone number).

* 1. General System Description
		1. DATA TYPES AND SENSITIVITY

List the types of data the system processes and the sensitivity of each data type with respect to confidentiality, integrity, and availability. Data sensitivity will be highly specific to the customer or mission needs. For example, a satellite mission serving multiple customers may have some customers with low confidentiality needs, and other customers whose data requires moderate or high confidentiality protections.

For illustrative purposes only, consider a hypothetical spacecraft. Likely data types would include:

* Spacecraft telecommands (low confidentiality, high integrity, high availability)
* Spacecraft telemetry (high confidentiality, high integrity, low availability)
* Data relay or rebroadcast data (low confidentiality, low integrity, moderate availability)
	+ 1. system criticality

The types of data listed in section above should be used to establish an overall criticality for the system that will influence default protections for components within the system’s security boundary.

* + 1. System Environment

Provide a general technical description of the system. Identify the primary hardware, software, and communications components.

* 1. System Interconnections
		1. Information Sharing

List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is a formal agreement to interconnect on file, the date of said agreement, data types exchanged, certification or accreditation status, and the authorizing official(s).

* + 1. Related Laws/Regulations/Policies

List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

* 1. Security Controls

Select an appropriate security control baseline, then provide a thorough description of how all the security controls in the applicable baseline are being implemented or planned to be implemented. The description should contain: 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3) any scoping guidance that has been applied and what type of consideration; and 4) indicate if the security control is a common control and who is responsible for its implementation.

* + 1. Space System Security Controls

As described in section 4.3, many of the ISO 27001 and related security controls from reference [6] may not be directly applicable in a space environment. Generic information technology frameworks commonly omit many concerns common to a space mission environment, and include many concerns pertinent to a generic information technology system but not applicable to a space mission environment. The security controls listed below in Table 1 are a set of controls that have been tailored to the most common needs of space systems, ground operations systems, and development facilities for spacecraft or ground systems. Each of these controls, numbered and grouped according to their related ISO 27001 subject areas (A.5, A.6, A.7, …), either references existing ISO 27001 controls that are also applicable to space missions, or else lists objectives specific to space missions that are absent from ISO 27001. These may be selected according to organizational needs to establish policies and system requirements, or recommend countermeasures to probable risks. These controls may also be used to augment other controls if compliance with other control frameworks are required by law or policy.

The security controls implemented for a particular system should take into consideration the entire duration of the mission, including pre- and post-flight periods. While different security controls may be appropriate for implementation during different mission phases, the overall selection of security controls for a mission should ensure that one phase’s protections (e.g., for confidentiality of proprietary data) are not nullified by vulnerabilities left unmitigated during other phases.

The mission planner should evaluate the applicability of each of the controls below to the mission needs and objectives. Where certain controls are considered inappropriate, the plan should document the reasons. Where certain controls are considered necessary for a mission even if not recommended below, the plan should include them and document the reasons. Some controls that have not been provided in previous space missions may need to be provided in future ones, due to the changes in system capabilities and the threat environment.

Table –Security Controls for Space Systems

| Control Number | Security Control Objective | Development Systems | Ground Operations Systems | Space Systems |
| --- | --- | --- | --- | --- |
| A.5 Security policy  |
| A.5.1 Information security policy  |
| A.5.1.MP1 | The ISO 27001 controls:* A.5.1.1 Information security policy document
* A.5.1.2 Review of the information security policy

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.5.1.MP2 | Security controls should give highest priority to the safe operation of the spacecraft, and the safety of the occupants in the case of manned spacecraft. |  | Y | Y |
| A.5.1.MP3 | Space systems should provide security controls to mitigate the safety risks to bystanders at expected launch and landing areas. |  | Y | Y |
| A.5.1.MP4 | Security controls for space systems should be designed so as not to inhibit mission accomplishment. A mission that places a higher priority on avoiding a security breach than on accomplishing the mission objectives should clearly state so in the mission security policy. |  | Y | Y |
| A.5.1.MP5 | Consideration should be given to employing security controls for space systems that are suitable for operations and maintenance throughout the duration of the mission lifecycle, to the extent known. (For example, selection of cryptographic methods should take into account the increasing computational resources available to potential attackers which may render current methods obsolete in time.) |  |  | Y – This control may be mitigated by anticipating a means of upgrading spacecraft flight software. |
| A.6 Organization of information security  |
| A.6.1 Internal organization  |
| A.6.1.MP1 | The ISO 27001 controls:* A.6.1.1 Management commitment to information security
* A.6.1.2 Information security coordination
* A.6.1.3 Allocation of information security responsibilities
* A.6.1.4 Authorization process for information processing facilities
* A.6.1.5 Confidentiality agreements
* A.6.1.6 Contact with authorities
* A.6.1.7 Contact with special interest groups

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.6.1.MP2 | The ISO 27001 control:* A.6.1.8 Independent review of information security

should be satisfied for all facilities and systems affiliated with a mission. A review conducted using a separate internal branch of the organisation may suffice in certain cases, if no qualified external organisation can be obtained to conduct the review. | Y | Y | Y |
| A.6.2 External parties  |
| A.6.2.MP1 | The ISO 27001 controls:* A.6.2.1 Identification of risks related to external parties
* A.6.2.2 Addressing security when dealing with customers
* A.6.2.3 Addressing security in third party agreements

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.7 Asset management  |
| A.7.1 Responsibility for assets  |
| A.7.1.MP1 | The ISO 27001 controls:* A.7.1.1 Inventory of assets
* A.7.1.2 Ownership of assets
* A.7.1.3 Acceptable use of assets

should be satisfied for all development and ground operations facilities. | Y | Y |  |
| A.7.2 Information classification  |
| A.7.2.MP1 | The ISO 27001 controls:* A.7.2.1 Classification guidelines
* A.7.2.2 Information labelling and handling

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.8 Human resources security  |
| A.8.1 Prior to employment  |
| A.8.1.MP1 | The ISO 27001 controls:* A.8.1.1 Roles and responsibilities
* A.8.1.2 Screening
* A.8.1.3 Terms and conditions of employment

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.8.2 During employment  |
| A.8.2.MP1 | The ISO 27001 controls:* A.8.2.1 Management responsibilities
* A.8.2.2 Information security awareness, education, and training
* A.8.2.3 Disciplinary process

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.8.3 Termination or change of employment  |
| A.8.3.MP1 | The ISO 27001 controls:* A.8.3.1 Termination responsibilities
* A.8.3.2 Return of assets
* A.8.3.3 Removal of access rights

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.9 Physical and environmental security  |
| A.9.1 Secure areas  |
| A.9.1.MP1 | The ISO 27001 controls:* A.9.1.1 Physical security perimeter
* A.9.1.2 Physical entry controls
* A.9.1.3 Securing offices, rooms and facilities
* A.9.1.4 Protecting against external and environmental threats
* A.9.1.5 Working in secure areas
* A.9.1.6 Public access, delivery, and loading areas

should be satisfied for all development and ground operations facilities. | Y | Y |  |
| A.9.2 Equipment security  |
| A.9.2.MP1 | The ISO 27001 controls:* A.9.2.1 Equipment siting and protection
* A.9.2.2 Supporting utilities
* A.9.2.3 Cabling security
* A.9.2.4 Equipment maintenance

should be satisfied for all ground operations facilities with telecommanding capability. |  | Y |  |
| A.9.2.MP2 | The ISO 27001 controls:* A.9.2.1 Equipment siting and protection
* A.9.2.4 Equipment maintenance

should be satisfied for all spacecraft processing facilities. Spacecraft and spacecraft components should be protected against unauthorized modification during pre-flight handling and storage. | Y |  |  |
| A.9.2.MP3 | The ISO 27001 controls:* A.9.2.5 Security of equipment off-premises
* A.9.2.6 Secure disposal or re-use of equipment
* A.9.2.7 Removal of property

should be satisfied for all development and ground operations facilities. | Y | Y |  |
| A.9.2.MP4 | Ground operations systems should provision for trajectory prediction and object tracking in order to predict potential collisions of the spacecraft with other objects. |  | Y |  |
| A.10 Communications and operations management  |
| A.10.1 Operational procedures and responsibilities  |
| A.10.1.MP1 | The ISO 27001 controls:* A.10.1.1 Documented operating procedures
* A.10.1.2 Change management

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.10.1.MP2 | The ISO 27001 control:* A.10.1.3 Segregation of duties

should be satisfied for all development and ground operations facilities. | Y | Y |  |
| A.10.1.MP3 | The ISO 27001 controls:* A.10.1.4 Separation of development, test and operational facilities

should be satisfied for all development and ground operations facilities. Systems should be designed to minimize access to operational components for purposes other than direct mission integration & operations (e.g., by providing data replication for indirect/offline mission support). | Y | Y |  |
| A.10.2 Third party service delivery management  |
| A.10.2.MP1 | The ISO 27001 controls:* A.10.2.1 Service delivery
* A.10.2.2 Monitoring and review of third party services
* A.10.2.3 Managing changes to third party services

should be satisfied for all systems.  | Y | Y | Y – This control should be satisfied for space systems where third-party services are used, e.g., for data relay. |
| A.10.3 System planning and acceptance  |
| A.10.3.MP1 | The ISO 27001 control:* A.10.3.1 Capacity management

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.10.3.MP2 | The ISO 27001 control:* A.10.3.2 System acceptance

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.10.4 Protection against malicious and mobile code  |
| A.10.4.MP1 | The ISO 27001 controls:* A.10.4.1 Controls against malicious code
* A.10.4.2 Controls against mobile code

should be satisfied for all development and ground operations facilities. | Y | Y | Y – This control should be satisfied for space systems where network protocols are used, depending upon the processing capabilities (onboard applications, network stack, etc.) of the spacecraft. |
| A.10.5 Back-up  |
| A.10.5.MP1 | The ISO 27001 control:* A.10.5.1 Information back-up

should be satisfied for all development and ground operations facilities. | Y | Y |  |
| A.10.6 Network security management  |
| A.10.6.MP1 | The ISO 27001 controls:* A.10.6.1 Network controls
* A.10.6.2 Security of network services

should be satisfied for all development and ground operations facilities. | Y | Y | Y – This control should be satisfied for space systems where network protocols are used. |
| A.10.7 Media handling  |
| A.10.7.MP1 | The ISO 27001 controls:* A.10.7.1 Management of removable media
* A.10.7.2 Disposal of media
* A.10.7.3 Information handling procedures
* A.10.7.4 Security of system documentation

should be satisfied for all development and ground operations facilities. | Y | Y |  |
| A.10.8 Exchange of information  |
| A.10.8.MP1 | The ISO 27001 controls:* A.10.8.1 Information exchange policies and procedures
* A.10.8.2 Exchange agreements
* A.10.8.3 Physical media in transit
* A.10.8.4 Electronic messaging
* A.10.8.5 Business information systems

should be satisfied for all facilities and systems affiliated with a mission. Sample processes and templates for documenting such agreements are described in reference . | Y | Y | Y – This control should be satisfied for space systems where third-party services (e.g., data relay services) are used. |
| A.10.8.MP2 | Consideration should be given to employing security controls that facilitate the use of cross-support within the mission's security policy. For example, the communications architecture may need to anticipate the possible occasional use of other organisations' RF ground stations. | Y | Y | Y |
| A.10.9 Electronic commerce services  |
| A.10.9.MP1 | The ISO 27001 controls:* A.10.9.1 Electronic commerce
* A.10.9.2 On-line transactions
* A.10.9.3 Publicly available information

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.10.10 Monitoring  |
| A.10.10.MP1 | The ISO 27001 controls:* A.10.10.1 Audit logging
* A.10.10.2 Monitoring system use
* A.10.10.3 Protection of log information
* A.10.10.4 Administrator and operator logs

should be satisfied for all ground operations facilities. | Y | Y | Y – This control should be satisfied for manned space systems if there is a need to attribute crew actions to particular individuals. |
| A.10.10.MP2 | The ISO 27001 control:* A.10.10.5 Fault logging

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y – Telemetry is the normal means of recording spacecraft events. |
| A.10.10.MP3 | All telecommand activity should be logged. | Y | Y | Y – Space systems may be unable to provide onboard logging of certain hardware-decoded, “essential” commands. |
| A.10.10.MP4 | The ISO 27001 control:* A.10.10.6 Clock synchronization

should be satisfied for all ground operations systems. |  | Y |  |
| A.10.10.MP5 | Space systems and ground systems should provide time synchronization capabilities in order to provide accurate situational awareness for coordinating operations. Spacecraft telemetry should provide indication of spacecraft internal time. Ground systems should calibrate the time reported in spacecraft telemetry. |  | Y – Ground systems should monitor the deviation of spacecraft internal clocks from ground-based time, accounting for expected transmission delays in receipt of telemetry. | Y |
| A.11 Access control  |
| A.11.1 Business requirement for access control  |
| A.11.1.MP1 | The ISO 27001 control:* A.11.1.1 Access control policy

should be satisfied for all development and ground operations facilities. | Y | Y |  |
| A.11.2 User access management  |
| A.11.2.MP1 | The ISO 27001 controls:* A.11.2.1 User registration
* A.11.2.2 Privilege management
* A.11.2.3 User Password management
* A.11.2.4 Review of user access rights

should be satisfied for all development and ground operations facilities. | Y | Y | Y – This control should be satisfied for manned space systems if there is a need to attribute crew actions to particular individuals. |
| A.11.3 User responsibilities  |
| A.11.3.MP1 | The ISO 27001 controls:* A.11.3.1 Password use
* A.11.3.2 Unattended user equipment
* A.11.3.3 Clear desk and clear screen policy

should be satisfied for all ground operations facilities. |  | Y | Y – This control should be satisfied for manned space systems if there is a need to attribute crew actions to particular individuals. |
| A.11.4 Network access control  |
| A.11.4.MP1 | The ISO 27001 controls:* A.11.4.1 Policy on use of network services
* A.11.4.2 User authentication for external connections
* A.11.4.3 Equipment identification in networks
* A.11.4.4 Remote diagnostic and configuration port protection
* A.11.4.5 Segregation in networks
* A.11.4.6 Network connection control
* A.11.4.7 Network routing control

should be satisfied for all development and ground operations facilities.  | Y | Y | Y – These controls should be satisfied for all space systems where networking protocols are used, particularly where mobile or ad-hoc networking is enabled. |
| A.11.4.MP2 | Space systems should provide segregation between critical vehicle communications and other in-flight communications or networking. Reference describes one potential architecture for providing such segregation. |  |  | Y |
| A.11.5 Operating system access control  |
| A.11.5.MP1 | The ISO 27001 controls:* A.11.5.1 Secure log-on procedures
* A.11.5.2 User identification and authorization
* A.11.5.3 Password management system
* A.11.5.4 Use of system utilities
* A.11.5.5 Session time-out
* A.11.5.6 Limitation of connection time

should be satisfied for all development and ground operations facilities. | Y | Y | Y – This control should be satisfied for manned space systems if there is a need to attribute crew actions to particular individuals. |
| A.11.6 Application and information access control  |
| A.11.6.MP1 | The ISO 27001 controls:* A.11.6.1 Information access restriction
* A.11.6.2 Sensitive system isolation

should be satisfied for all development and ground operations facilities. | Y | Y |  |
| A.11.6.MP2 | Space systems should provide a dedicated (isolated) computing environment for critical vehicle control functions, separate from that used for other in-flight computing functions. |  |  | Y |
| A.11.7 Mobile computing and teleworking  |
| A.11.7.MP1 | The ISO 27001 controls:* A.11.7.1 Mobile computing and communications
* A.11.7.2 Teleworking

should be satisfied for all development and ground operations facilities. | Y | Y |  |
| A.12 Information systems acquisition, development and maintenance  |
| A.12.1 Security requirements of information systems  |
| A.12.1.MP1 | The ISO 27001 control:* A.12.1.1 Security requirements analysis and specification

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.12.2 Correct processing in applications  |
| A.12.2.MP1 | The ISO 27001 controls:* A.12.2.1 Input data validation
* A.12.2.2 Control of internal processing
* A.12.2.3 Message integrity
* A.12.2.4 Output data validation

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.12.2.MP2 | Space systems should detect the loss, re-sequencing, or attempted replay of received telecommands. |  |  | Y |
| A.12.2.MP3 | Space systems should provide the capability to authorize execution of individual telecommands according to a defined time window. |  |  | Y |
| A.12.2.MP4 | Ground systems should detect the loss or data corruption of received telemetry. |  | Y |  |
| A.12.3 Cryptographic controls  |
| A.12.3.MP1 | The ISO 27001 controls:* A.12.3.1 Policy on the use of cryptographic controls
* A.12.3.2 Key management

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.12.3.MP2 | Space systems and ground systems should provide cryptographic authentication in order to protect telecommands. Keyed authentication should be used so that the receiving end can verify the identity of the source and the data integrity of the telecommand. | Y | Y | Y |
| A.12.3.MP3 | Space systems and ground systems should provide for encryption in order to ensure the confidentiality (where required by policy) of telecommands, telemetry, audio, and video data. | Y | Y | Y |
| A.12.3.MP4 | Space systems and ground systems should use cryptographic components (including software, where appropriate) that have been validated for correctness by an external third party according to recognized criteria (e.g., Common Criteria or FIPS 140). | Y | Y | Y |
| A.12.3.MP5 | Space systems and ground systems should protect cryptographic keys used for telecommands and telemetry against key recovery by unauthorized parties. | Y | Y | Y |
| A.12.4 Security of system files  |
| A.12.4.MP1 | The ISO 27001 controls:* A.12.4.1 Control of operational software
* A.12.4.2 Protection of system test data
* A.12.4.3 Access control to program source code

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.12.5 Security in development and support processes  |
| A.12.5.MP1 | The ISO 27001 controls:* A.12.5.1 Change control procedures
* A.12.5.2 Technical review of applications after operating system changes
* A.12.5.3 Restrictions on changes to software packages
* A.12.5.5 Outsourced software development

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.12.5.MP2 | The ISO 27001 control:* A.12.5.4 Information leakage

should be satisfied for all facilities and systems affiliated with a mission. Systems should restrict the dissemination of detailed spacecraft ground test procedures and configurations. | Y | Y | Y |
| A.12.5.MP3 | Spacecraft ground test configurations should validate the correct operation of security controls for spacecraft communications (especially for telecommands and telemetry). | Y | Y | Y |
| A.12.6 Technical vulnerability management  |
| A.12.6.MP1 | The ISO 27001 control:* A.12.6.1 Control of technical vulnerabilities

should be satisfied for all facilities and systems affiliated with a mission. Security controls should be reviewed periodically for obsolescence and the discovery of technical vulnerabilities. The system’s security policy should define the frequency of reviews. | Y | Y | Y |
| A.13 Information security incident management  |
| A.13.1 Reporting information security events and weaknesses  |
| A.13.1.MP1 | The ISO 27001 controls:* A.13.1.1 Reporting information security events
* A.13.1.2 Reporting security weaknesses

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.13.2 Management of information security incidents and improvements  |
| A.13.2.MP1 | The ISO 27001 controls:* A.13.2.1 Responsibilities and procedures
* A.13.2.2 Learning from information security incidents
* A.13.2.3 Collection of evidence

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.13.2.MP2 | Space systems should have a policy for handling recovery/disposal of flight hardware and/or debris. |  |  | Y |
| A.14 Business continuity management  |
| A.14.1 Information security aspects of business continuity management  |
| A.14.1.MP1 | The ISO 27001 controls:* A.14.1 Including information security in the business continuity management process
* A.14.2 Business continuity and risk assessment
* A.14.3 Developing and implementing continuity plans including information security
* A.14.4 Business continuity planning framework
* A.14.5 Testing, maintaining and re-assessing business continuity plans

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.14.1.MP2 | Space systems and ground systems should define availability requirements, and provide redundancy in systems and/or components as necessary to meet the defined availability levels. | Y | Y | Y |
| A.14.1.MP3 | Space systems and ground systems should ensure that security controls are re-established following a recovery from a failure or an interruption of communications. | Y | Y | Y |
| A.14.1.MP4 | Space systems operating in a “safe mode”, or in a degraded capacity where security controls may be nonfunctioning, should permit only a limited set of telecommands until the system is returned to nominal operations. |  |  | Y |
| A.15 Compliance  |
| A.15.1 Compliance with legal requirements  |
| A.15.1.MP1 | The ISO 27001 controls:* A.15.1.1 Identification of applicable legislation
* A.15.1.2 Intellectual property rights (IPR)
* A.15.1.3 Protection of organizational records
* A.15.1.4 Data protection and privacy of personal information
* A.15.1.5 Prevention of misuse of information processing facilities
* A.15.1.6 Regulation of cryptographic controls

should be satisfied for all facilities and systems affiliated with a mission. The mission security policy should define which are the applicable laws, regulations, and policies for the mission. | Y | Y | Y |
| A.15.1.MP2 | Missions having international scope should provide for operation of cryptographic controls in accordance with export/import restrictions and national laws. The mission security policy should define which are the applicable laws, regulations, and policies for the mission. | Y | Y | Y |
| A.15.2 Compliance with security policies and standards, and technical compliance  |
| A.15.2.MP1 | The ISO 27001 controls:* A.15.2.1 Compliance with security policy
* A.15.2.2 Technical compliance checking

should be satisfied for all facilities and systems affiliated with a mission. | Y | Y | Y |
| A.15.3 Information systems audit considerations  |
| A.15.3.MP1 | The ISO 27001 controls:* A.15.3.1 Information systems audit controls
* A.15.3.2 Protection of information systems audit tools

should be satisfied for all development and ground operations facilities. | Y | Y |  |

1. Informative References
2. *Space Missions Key Management Concept*. Informational Report, CCSDS 350.6-G-0. Green Book. Washington, D.C.: CCSDS, \_\_\_\_.
3. *CCSDS Security Algorithms*. Recommendation for Space Data System Standards, CCSDS 352.0-R-0. Red Book. Washington, D.C.: CCSDS, \_\_\_\_\_.
4. *Space Data Link Security Protocol*. Recommendation for Space Data System Standards, CCSDS 355.0-R-1. Red Book. Washington, D.C.: CCSDS, 2010.
5. *Space Data Link Security Concept of Operation*. Informational Report, CCSDS 350.5-G-1. Green Book. Washington, D.C.: CCSDS, \_\_\_\_\_.
6. *Recommended Security Controls for Federal Information Systems and Organizations*. National Institute of Standards and Technology Special Publication 800-53. Revision 3. Gaithersburg, Maryland: NIST, August 2009.
7. *Guide for Mapping Types of Information and Information Systems to Security Categories*. National Institute of Standards and Technology Special Publication 800-60. Revision 2. Gaithersburg, Maryland: NIST, June 2004.
8. *COBIT® 4.1*. IT Governance Institute, 2007.
9. *Commercial Aircraft Information Security Concepts of Operation and Process Framework*. ARINC Report 811. Aeronautical Radio Inc., December 2005.

NOTE: Normative references are listed in section .