[COMPANY NAME]

Complex Commercial SATCOM Solutions (CS3)
Risk Management Framework Plan (RMFP)

Prepared for:

GSA ISSM

1800 F STREET, NW
WASHINGTON, DC 20405

Prepared by:

[CONTACT INFORMATION]

[ADDRESS]

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Initial Version – <Date>				
Revision 1 - <Date>				
1	<Name>	<Change>	<Reason for change>	<Page>

Table of Contents

List of Figures

Executive Overview

1. Introduction

Organizations depend on information technology and the information systems that are developed from that technology to successfully carry out their missions and business functions. Information systems can include as constituent components, a range of diverse computing platforms from high-end supercomputers to personal digital assistants and cellular telephones. Information systems can also include very specialized systems and devices (e.g., satellite communications systems).

Federal information and information systems and nonfederal systems and organizations are subject to serious threats that can have adverse impacts on organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation by compromising the confidentiality, integrity, or availability of information being processed, stored, or transmitted by those systems. Threats to information and information systems which include environmental disruptions, human or machine errors, and purposeful attacks can directly impact the ability of the federal government to successfully conduct its assigned missions and business operations.

Cyber-attacks on information systems today are often aggressive, disciplined, well-organized, well-funded, and in a growing number of documented cases, very sophisticated. Successful attacks on public and private sector information systems can result in serious or grave damage to the national and economic security interests of the United States. Given the significant and growing danger of these threats, it is imperative that leaders at all levels of an organization understand their responsibilities for achieving adequate information security and for managing information system-related security risks.

1.1 Purpose

The National Institute of Standards and Technology (NIST) working with the Department of Defense and other organizations developed a common information security framework for the Federal Government and its contractors. The Risk Management Framework (RMF) transitions from the traditional certification and accreditation (C&A) process to an assessment and authorization (A&A) process and includes a continuous monitoring process.

The Risk Management Framework Plan (RMFP) describes the <**Company Name**> approach for <**Company Name/System Name**> security compliance with the General Services Administration (GSA) Complex Commercial SATCOM Solutions (CS3) security requirements. It defines the integration of the RMF with the System Development Life Cycle (SDLC) for Commercial Satellite Communications (COMSATCOM) services delivered.

1.2 Scope

The RMF process is followed by <**Company Name>. Describe how the RMF process is applied.**

1.3 Roles and Responsibilities

There are many roles associated with the RMF process. System Owners for each information system are responsible for ensuring their respective systems utilized for delivery of COMSATCOM service have been through the GSA RMF process. The following sections provide a high level description of the primary positions/roles within the organization who execute management and operational RMF process responsibilities.

1.3.1 Company position with ultimate responsibility

Describe the security risk management responsibilities assigned to the Chief Executive Officer (CEO)/President/etc.

1.3.2 Other company positions with responsibility for information system security

(Add as many positions as required.)

Describe the information system-related security risk management roles and responsibilities assigned to other personnel within the organization

2. Integrated Organization-Wide Risk Management

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance.**

Replace the text within the brackets [].

[*Managing information system-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization—from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning and managing projects, to individuals on the front lines developing, implementing, and operating the systems supporting the organization's core missions and business processes. Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization. Figure 2-1 illustrates a three-tiered approach to risk management that addresses risk-related concerns at: (i) the organization level; (ii) the mission and business process level; and (iii) the information system level.*

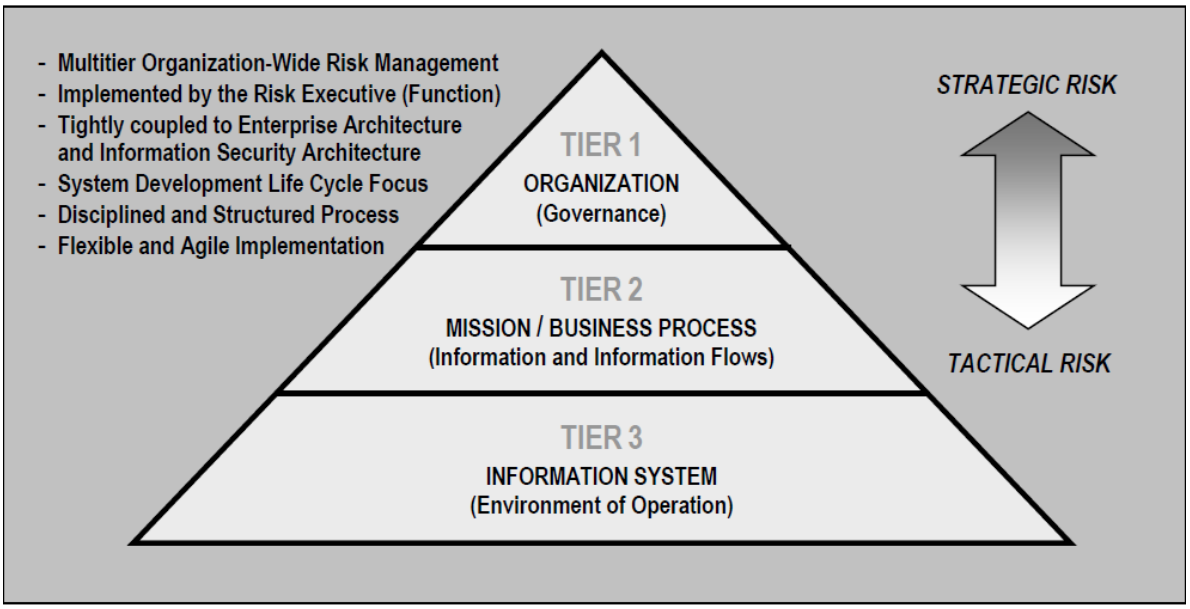

Figure 2-1. Tiered Risk Management Approach Example (*NIST SP 800-37)*

***Tier 1** addresses risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy that includes: (i) the techniques and methodologies the organization plans to employ to assess information system-related security risks and other types of risk of concern to the organization; (ii) the methods and procedures the organization plans to use to evaluate the significance of the risks identified during the risk assessment; (iii) the types and extent of risk mitigation measures the organization plans to employ to address identified risks; (iv) the level of risk the organization plans to accept (i.e., risk tolerance); (v) how the organization plans to monitor risk on an ongoing basis given the inevitable changes to organizational information systems and their environments of operation; and (vi) the degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out.*

***Tier 2** addresses risk from a mission and business process perspective and is guided by the risk decisions at Tier 1. Tier 2 activities are closely associated with enterprise architecture and include: (i) defining the core missions and business processes for the organization (including any derivative or related missions and business processes carried out by subordinate organizations); (ii) prioritizing missions and business processes with respect to the goals and objectives of the organization; (iii) defining the types of information that the organization needs to successfully execute the stated missions and business processes and the information flows both internal and external to the organization; (iv) developing an organization-wide information protection strategy and incorporating high-level information security requirements into the core missions and business processes; and (v) specifying the degree of autonomy for subordinate organizations (i.e., organizations within the parent organization) that the parent organization permits for assessing, evaluating, mitigating, accepting, and monitoring risk.*

Because subordinate organizations responsible for carrying out derivative or related missions and business processes may have already invested in their own methods of assessing,

evaluating, mitigating, accepting and monitoring risk, parent organizations may allow a greater degree of autonomy within parts of the organization or across the entire organization in order to minimize costs.

***Tier 3** addresses risk from an information system perspective and is guided by the risk decisions at Tiers 1 and 2. Risk decisions at Tiers 1 and 2 impact the ultimate selection and deployment of needed safeguards and countermeasures (i.e., security controls) at the information system level. Information security requirements are satisfied by the selection of appropriate management, operational, and technical security controls. The security controls are subsequently allocated to the various components of the information system as system-specific, hybrid, or common controls in accordance with the information security architecture developed by the organization. Security controls are typically traceable to the security requirements established by the organization to ensure that the requirements are fully addressed during design, development, and implementation of the information system. Security controls can be provided by the organization or by an external provider.*]

3. Risk Management Framework Process

The below text with **red font** provides additional guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies the RMF process to various infrastructure functions provided to the client agencies such as network connectivity, cloud services, managed network and managed security services.**

Replace the text within the brackets [].

[*The Risk Management Framework (RMF), illustrated in Figure 3-1, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The RMF operates primarily at Tier 3 in the risk management hierarchy but can also have interactions at Tiers 1 and 2 (e.g., providing feedback from ongoing authorization decisions to the risk executive [function], dissemination of updated threat and risk information to authorizing officials*[1] *and information system owners). The RMF integrates the security life cycle with the risk life cycle of the system development process. The RMF steps include:*

- ***Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis.*
- ***Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.*
- ***Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.*
- ***Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and*

[1] NIST 800-37 The role of Authorizing Official has inherent U.S. Government authority and is assigned to Government personnel only.

producing the desired outcome with respect to meeting the security requirements for the system.

- ***Authorize** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.*[2]
- ***Monitor** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.*]

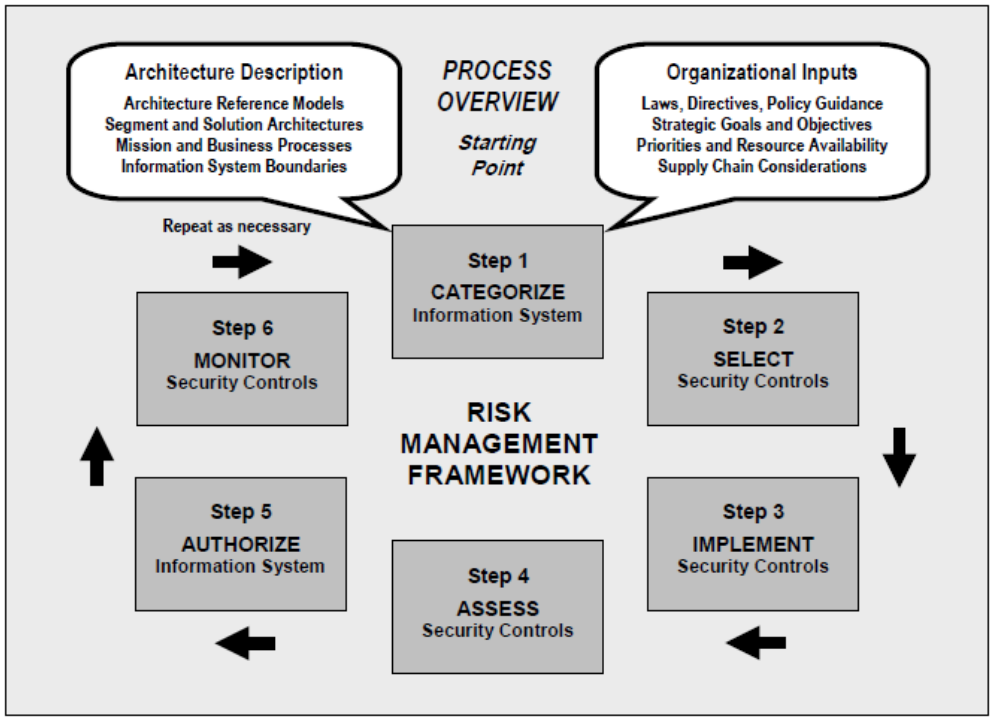

Figure 3-1. The NIST RMF Lifecycle, per NIST SP 800-37

Note: The Organization's Risk Management Framework Plan should include processes and procedures to accomplish all of the steps identified in Figure 3-1, except Authorize. For COMSATCOM service providers, the Authorize step is more appropriately defined as an approval for system operations with other service providers (e.g., satellite operators, satellite operations centers, etc.).

[2] NIST 800-37 Security Authorization is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizations operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

3.1 RMF Step 1 – Categorize Information System

3.1.1 Security Categorization

The overall Federal Information Processing Standards Publication (FIPS) 199 security categorization standards were reviewed by GSA in order to assign an accurate security categorization level for the information and information systems for CS3 COMSATCOM services delivered to the Government. GSA has determined the CS3 Commercial Satellite Communications (COMSATCOM) systems and components to include the Satellite, Ground Station/Telemetry and/or the Operations/Business Support System, have an overall security categorization rating of **Moderate**.

The Contractor's information assurance boundary is where the Offeror's services connect to the user terminals/equipment (i.e., includes satellite, telemetry (including command encryption for ground and space); Operations/Business Support systems used in the Satellite Operations Centers (SOCs), Network Operations Centers (NOCs), and teleport(s).

3.1.2 Information System Description

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to describe the information system (including system boundary) and documents the description in the organization's security plan.**

Note: The <Company Name> will provide the Table of Contents for their Security Plan as Appendix B to provide the Government with insight into the quality and depth of the Security Plan.

Replace the text within the brackets [].

[*Supplemental Guidance: Descriptive information about the information system is documented in the system identification section of the security plan, included in attachments to the plan, or referenced in other standard sources. The level of detail provided in the security plan is determined by the organization and is typically commensurate with the security categorization of the information system. Information may be added to the system description as it becomes available during the system development life cycle and execution of the RMF tasks. A system description may include, for example:*

- *Full descriptive name of the information system including associated acronym;*
- *Unique information system identifier (typically a number or code);*
- *Information system owner including contact information;*
- *Parent or governing organization that manages, owns, and/or controls the information system;*
- *Location of the information system and environment in which the system operates;*
- *Version or release number of the information system;*
- *Purpose, functions, and capabilities of the information system and missions/business processes supported;*
- *How the information system is integrated into the enterprise architecture and information security architecture;*

- *Results of the security categorization process for the information and information system;*
- *Types of information processed, stored, and transmitted by the information system;*
- *Boundary of the information system for risk management and security authorization purposes;*
- *Applicable laws, directives, policies, regulations, or standards affecting the security of the information system;*
- *Architectural description of the information system including network topology;*
- *Hardware and firmware devices included within the information system;*
- *System and applications software resident on the information system;*
- *Hardware, software, and system interfaces (internal and external);*
- *Subsystems (static and dynamic) associated with the information system;*
- *Information flows and paths (including inputs and outputs) within the information system;*
- *Cross domain devices/requirements;*
- *Network connection rules for communicating with external information systems;*
- *Interconnected information systems and identifiers for those systems;*
- *Encryption techniques used for information processing, transmission, and storage;*
- *Cryptographic key management information (public key infrastructures, certificate authorities, etc.);*
- *Information system users (including organizational affiliations, access rights, privileges);*
- *Ownership/operation of information system*
- *Incident response points of contact; and*
- *Other information as required by the organization*]

3.2 RMF Step 2 – Select Security Controls

3.2.1 Common Control Identification

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).**

Replace the text within the brackets [].

[*Supplemental Guidance: Common controls (e.g., physical and environmental protection controls, personnel security controls) are security controls that are inherited by one or more organizational information systems. Common controls are identified and assigned to specific organizational entities (designated as common control providers) for development, implementation, assessment, and monitoring. Common control providers may also be information system owners when the common controls are resident within an information system. The organization consults information system owners when identifying common controls to ensure that the security capability provided by the inherited controls is sufficient to deliver adequate protection. When the common controls provided by the organization are not sufficient for information systems inheriting the controls, the system owners supplement the*

common controls with system-specific or hybrid controls to achieve the required protection for the system and/or accept greater risk. Common control providers are responsible for: (i) documenting common controls in a security plan (or equivalent document prescribed by the organization); (ii) ensuring that common controls are developed, implemented, and assessed for effectiveness by qualified assessors with a level of independence required by the organization; (iii) documenting assessment findings in a security assessment report; (iv) producing a plan of action and milestones for all common controls deemed less than effective (i.e., having unacceptable weaknesses or deficiencies in the controls); and (v) monitoring common control effectiveness on an ongoing basis.

Organizations ensure that common control providers have the capability to rapidly broadcast changes in the status of common controls that adversely affect the protections being provided by and expected of the common controls. Common control providers are able to quickly inform information system owners when problems arise in the inherited common controls (e.g., when an assessment or reassessment of a common control indicates the control is flawed in some manner, when a new threat or attack method arises that renders the common control less than effective in protecting against the new threat or attack method).]

3.2.2 Security Control Selection

The security control selection for CS3 COMSATCOM services has been completed by GSA. In relation to the components included within the COMSATCOM system boundaries; (e.g., the Satellite, the Ground Station/Telemetry and / or the Operations or Business Support Systems, the security controls that must be implemented have been derived from the NIST 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. Appendix A is the Information Assurance Checklist Template for CS3 COMSATCOM Task Orders.

3.2.3 Monitoring Strategy

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation.**

Replace the text within the brackets [].

[*Supplemental Guidance: A critical aspect of risk management is the ongoing monitoring of security controls employed within or inherited by the information system. The implementation of a robust continuous monitoring program allows an organization to understand the security state of the information system over time and maintain the initial security authorization in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business functions. The ongoing monitoring of security controls using automated tools and supporting databases facilitates near real-time risk management for the information system. An effective monitoring program includes: (i) configuration management and control processes; (ii) security impact analyses on proposed or actual changes to the information system and its environment of operation; (iii) assessment of security controls employed within and inherited by the information system (including controls in dynamic subsystems); and (iv) security*

status reporting to appropriate organizational officials. The continuous monitoring strategy for the information system identifies the security controls to be monitored, the frequency of monitoring, and the control assessment approach. The strategy defines how changes to the information system will be monitored, how security impact analyses will be conducted, and the security status reporting requirements including recipients of the status reports.

Determining the frequency for assessing security controls inherited by the information system (i.e., common controls) includes the organization's determination of the trustworthiness of the common control provider. An organizational assessment of risk (either formal or informal) can also be used to guide the frequency of monitoring. The monitoring of security controls continues throughout the system development life cycle.]

3.2.4 Security Plan Approval

Note: For CS3, the Security Plan Approval process has been replaced by the Information Assurance Checklist Approval.

As related to the Satellites, Ground Stations/Telemetries and / or Operations/Business Support Systems within the COMSATCOM boundaries, for each CS3 COMSATCOM Task Order the Company must complete an Information Assurance (IA) Checklist. This checklist is a means to notate specifically how the pre-selected security controls are implemented within all applicable system environments. This checklist is provided in Appendix A of this document.

3.3 RMF Step 3 – Implement Security Controls

3.3.1 Security Control Implementation

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to implement the security controls specified in the Information Assurance (IA) checklist completed for each CS3 COMSATCOM Task Order.**

Replace the text within the brackets [].

[*Supplemental Guidance: Security control implementation is consistent with the organization's enterprise architecture and information security architecture. The information security architecture serves as a resource to allocate security controls (including, for example, security mechanisms and services) to an information system and any organization-defined subsystems. Security controls targeted for deployment within the information system (including subsystems) are allocated to specific system components responsible for providing a particular security capability. Not all security controls need to be allocated to every subsystem. Allocating some security controls as common controls or hybrid controls is part of this architectural process. Organizations use best practices when implementing the security controls within the information system including system and software engineering methodologies, security engineering principles, and secure coding techniques. In addition, organizations ensure that mandatory configuration settings are established and implemented on information technology products in accordance with federal and organizational policies.*]

3.3.2 Security Control Documentation

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to document the security control implementation in the security plan or other document, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).**

Replace the text within the brackets [].

[*Supplemental Guidance: Security control documentation describes how system-specific, hybrid, and common controls are implemented. The documentation formalizes plans and expectations regarding the overall functionality of the information system. The functional description of the security control implementation includes planned inputs, expected behavior, and expected outputs where appropriate, typically for those technical controls that are employed in the hardware, software, or firmware components of the information system. Documentation of security control implementation allows for traceability of decisions prior to and after deployment of the information system. The level of effort expended on documentation of the information system is commensurate with the purpose, scope, and impact of the system with respect to organizational missions, business functions, and operations. To the extent possible, organizations reference existing documentation (either by vendors or other organizations that have employed the same or similar information systems), use automated support tools, and maximize communications to increase the overall efficiency and cost effectiveness of security control implementation.***]**

3.4 RMF Step 4 – Assess Security Controls

3.4.1 Assessment Preparation

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to develop, review and approve the security assessment plan or similar document.**

Replace the text within the brackets [].

[*Supplemental Guidance: The security assessment plan provides the objectives for the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures. The security assessment plan is reviewed and approved by appropriate organizational officials to ensure that the plan is consistent with the security objectives of the organization, employs state-of-the practice tools, techniques, procedures, and automation to support the concept of continuous monitoring and near real-time risk management, and is cost-effective with regard to the resources allocated for the assessment. The purpose of the security assessment plan approval is two-fold: (i) to establish the appropriate expectations for the security control assessment; and (ii) to bound the level of effort for the security control assessment.*

Organizations consider both the technical expertise and level of independence required in selecting security control assessors. Organizations also ensure that security control assessors

possess the required skills and technical expertise to successfully carry out assessments of system-specific, hybrid, and common controls. This includes knowledge of and experience with the specific hardware, software, and firmware components employed by the organization. An independent assessor is any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system.]

3.4.2 Security Control Assessment

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to assess the security controls in accordance with the assessment procedures defined in the security assessment plan or similar document.**

Replace the text within the brackets [].

[*Supplemental Guidance: Security control assessments determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.*

The information system owner relies on the technical expertise and judgment of assessors to: (i) assess the security controls employed within or inherited by the information system using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and reduce or eliminate identified vulnerabilities. The assessor findings are an unbiased, factual reporting of the weaknesses and deficiencies discovered during the security control assessment.

The organization ensures that the assessors have access to: (i) the information system and environment of operation where the security controls are employed; and (ii) the appropriate documentation, records, artifacts, test results, and other materials needed to assess the security controls.

When security controls are provided to an organization by an external provider, the organization ensures that the assessors have access to the information system/environment of operation where the controls are employed as well as appropriate information needed to carry out the assessment. The organization also obtains any information related to existing assessments that may have been conducted by the external provider and reuses such assessment information whenever possible in accordance with the reuse criteria established by the organization. Descriptive information about the information system is typically documented in the system identification section of the security plan or included by reference or as attachments to the plan. Supporting materials such as procedures, reports, logs, and records showing evidence of security control implementation are identified as well. In order to make the risk management process as timely and cost-effective as possible, the reuse of previous assessment results, when reasonable and appropriate, is strongly recommended.]

3.4.3 Security Assessment Report

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to prepare the security assessment**

report documenting the issues, findings, and recommendations from the security control assessment.

Replace the text within the brackets [].

[*Supplemental Guidance: The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the security assessment report. The assessment report includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the assessor's findings.*

*The security control assessment report is an evolving document that includes assessment results from all relevant phases of the system development life cycle including the results generated during continuous monitoring. Organizations may choose to develop an executive summary from the detailed findings that are generated during a security control assessment. An executive summary provides an abbreviated version of the assessment report focusing on the highlights of the assessment, synopsis of key findings, and/or recommendations for addressing weaknesses and deficiencies in the security controls.***]**

3.4.4 Remediation Actions

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.**

Replace the text within the brackets [].

[*Supplemental Guidance: The security assessment report provides visibility into specific weaknesses and deficiencies in the security controls employed within or inherited by the information system. Such weaknesses and deficiencies are potential vulnerabilities if exploitable by a threat source. The findings generated during the security control assessment provide important information that facilitates a disciplined and structured approach to mitigating risks in accordance with organizational priorities. An updated assessment of risk (either formal or informal) based on the results of the findings produced during the security control assessment and any inputs from the risk executive (function), helps to determine the initial remediation actions and the prioritization of such actions.*

Organizations review assessor findings and determine the severity or seriousness of the findings (i.e., the potential adverse impact on organizational operations and assets, individuals, other organizations, or the Nation) and whether the findings are sufficiently significant to be worthy of further investigation or remediation. If weaknesses or deficiencies in security controls are corrected, the security control assessor reassesses the remediated controls for effectiveness. Security control reassessments determine the extent to which the remediated controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The security plan is updated based on the findings of the security control assessment and any remediation actions taken. The updated security plan reflects the actual state of the security controls after the initial

assessment and any modifications by the information system owner or common control provider in addressing recommendations for corrective actions. At the completion of the assessment, the security plan contains an accurate list and description of the security controls implemented (including compensating controls) and a list of residual vulnerabilities.]

3.5 RMF Step 5 – Authorize Information System

The security authorization step is an inherent federal responsibility that is directly linked to the management of risk related to the use of external information system services. **Please read the supplemental guidance found within Section 3.5 for understanding only - <Company Name> is not required to provide any input for Step 5 in their Risk Management Framework Plan.**

The below text with **red font** from NIST SP 800-37 provides an overview of the processes in the security authorization step. The security information (i.e., Information Assurance Checklist) submitted by the COMSATCOM service providers in response to a Task Order Request for Proposal is assessed by the Federal Government during the completion of Step 5 (Authorization of the Information System) process and procedures. After review of the information security documentation provided by COMSATCOM service providers, additional documentation (e.g., Security Plan contents or Security Assessments) may be requested for review by the Authorizing Official prior to the decision for authorization to operate the information system(s).

3.5.1 Plan of Action and Milestones

Supplemental Guidance: The plan of action and milestones, prepared for the authorizing official, is one of three key documents in the security authorization package and describes the specific tasks that are planned: (i) to correct any weaknesses or deficiencies in the security controls noted during the assessment; and (ii) to address the residual vulnerabilities in the information system. The plan of action and milestones identifies: (i) the tasks to be accomplished with a recommendation for completion either before or after information system implementation; (ii) the resources required to accomplish the tasks; (iii) any milestones in meeting the tasks; and (iv) the scheduled completion dates for the milestones. The plan of action and milestones is used by the authorizing official to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment. All security weaknesses and deficiencies identified during the security control assessment are documented in the security assessment report to maintain an effective audit trail.

3.5.2 Security Authorization Package

Supplemental Guidance: The security authorization package contains: (i) the security plan; (ii) the security assessment report; and (iii) the plan of action and milestones. The information in these key documents is used by authorizing officials to make risk-based authorization decisions. For information systems inheriting common controls for specific security capabilities, the security authorization package for the common controls or a reference to such documentation is also included in the authorization package. When security controls are provided to an organization by an external provider, the organization ensures that the information needed for authorizing officials to make risk-based decisions, is made available by the provider.

3.5.3 Risk Determination

Supplemental Guidance: The authorizing official assesses the information provided by the information system owner or common control provider regarding the current security state of the system or the common controls inherited by the system and the recommendations for addressing any residual risks. Risk assessments (either formal or informal) are employed at the discretion of the organization to provide needed information on threats, vulnerabilities, and potential impacts as well as the analyses for the risk mitigation recommendations. Risk-related information includes the criticality of organizational missions and/or business functions supported by the information system and the risk management strategy for the organization. After risk determination, organizations can respond to risk in a variety of ways, including: (i) accepting risk; (ii) avoiding risk; (iii) mitigating risk; (iv) sharing risk; (v) transferring risk; or (vi) a combination of the above. A key part of the risk decision process is the recognition that regardless of the risk decision, there typically remains a degree of residual risk. Organizations determine acceptable degrees of residual risk based on organizational risk tolerance.

3.5.4 Risk Acceptance

Supplemental Guidance: The authorizing official considers many factors when deciding if the risk to organizational operations (including mission, function, image, or reputation), organizational assets, individuals, other organizations, and the Nation, is acceptable. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision. The authorizing official issues an authorization decision for the information system and the common controls inherited by the system after reviewing all of the relevant information and, where appropriate, consulting with other organizational officials. Security authorization decisions are based on the content of the security authorization package and, where appropriate, any inputs received from key organizational officials. The authorization package provides relevant information on the security state of the information system including the ongoing effectiveness of the security controls employed within or inherited by the system.

The authorization decision document conveys the final security authorization decision from the authorizing official to the information system owner or common control provider, and other organizational officials, as appropriate. The authorization decision document contains the following information: (i) authorization decision; (ii) terms and conditions for the authorization; and (iii) authorization termination date. The security authorization decision indicates to the information system owner whether the system is: (i) authorized to operate; or (ii) not authorized to operate. The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider. The authorization termination date, established by the authorizing official, indicates when the security authorization expires.

3.6 RMF Step 6 – Security Control Monitoring

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to determine the security impact**

of proposed or actual changes to the information system and its environment of operation during the system Operation/Maintenance lifecycle phase.

Replace the text within the brackets [].

[*Supplemental Guidance: Information systems are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and operate. Strict configuration management and control processes are established by the organization to support such monitoring activities. It is important to record any relevant information about specific changes to hardware, software, or firmware such as version or release numbers, descriptions of new or modified features/capabilities, and security implementation guidance. It is also important to record any changes to the environment of operation for the information system (e.g., modifications to hosting networks and facilities, mission/business use of the system, threats), or changes to the organizational risk management strategy.*

Security impact analysis conducted by the organization, determines the extent to which proposed or actual changes to the information system or its environment of operation can affect or have affected the security state of the system. Changes to the information system or its environment of operation may affect the security controls currently in place (including system-specific, hybrid, and common controls), produce new vulnerabilities in the system, or generate requirements for new security controls that were not needed previously. If the results of the security impact analysis indicate that the proposed or actual changes can affect or have affected the security state of the system, corrective actions are initiated and appropriate documents revised and updated (e.g., the security plan).

*Most routine changes to an information system or its environment of operation can be handled by the organization's continuous monitoring program. Conducting security impact analyses is part of an ongoing assessment of risk. As risk assessments are updated and refined, organizations use the results to modify security plans based on the most recent threat and vulnerability information available. Updated risk assessments provide a foundation for prioritizing/planning risk responses.***]**

3.6.1 Ongoing Security Control Assessments

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to assess the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy during the system Operation/Maintenance lifecycle phase.**

Replace the text within the brackets [].

[*Supplemental Guidance: Subsequent to the initial authorization (i.e., during continuous monitoring), the organization assesses all security controls (including management, operational, and technical controls) employed within and inherited by the information system on an ongoing basis. The frequency of monitoring is based on the monitoring strategy developed by the information system owner or common control provider. Security control assessments in support*

of initial and subsequent security authorizations are conducted by independent assessors. Assessor independence during continuous monitoring, although not mandated, introduces efficiencies into the process and allows for reuse of assessment results in support of ongoing authorization and when reauthorization is required.]

3.6.2 Ongoing Remediation Actions

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones during the system Operation/Maintenance lifecycle phase.**

Replace the text within the brackets [].

[*Supplemental Guidance: The assessment information produced by an assessor during continuous monitoring is provided to the information system owner and common control provider in an updated security assessment report. The information system owner and common control provider initiate remediation actions on outstanding items listed in the plan of actions and milestones and findings produced during the ongoing monitoring of security controls. The security control assessor may provide recommendations as to appropriate remediation actions. An assessment of risk (either formal or informal) informs organizational decisions with regard to conducting ongoing remediation actions. Security controls that are modified, enhanced, or added during the continuous monitoring process are reassessed by the assessor to ensure that appropriate corrective actions are taken to eliminate weaknesses or deficiencies or to mitigate the identified risk.*]

3.6.3 Key Updates

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to update the security plan, security assessment report, or similar document based on the results of the continuous monitoring process during the system Operation/Maintenance lifecycle phase.**

Replace the text within the brackets [].

[*Supplemental Guidance: To facilitate the near real-time management of risk associated with the operation and use of the information system, the organization updates the security plan, security assessment report, and plan of action and milestones on an ongoing basis. The updated security plan reflects any modifications to security controls based on risk mitigation activities carried out by the information system owner or common control provider. The updated security assessment report reflects additional assessment activities carried out to determine security control effectiveness based on modifications to the security plan and deployed controls. The updated plan of action and milestones: (i) reports security impact analysis or security control monitoring; and (iii) describes how the information system owner or common control provider intends to address those vulnerabilities.*

The frequency of updates to risk management-related information is at the discretion of the information system owner, common control provider, and authorizing officials in accordance with federal and organizational policies.

When updating key information in security plans, security assessment reports, and plans of action and milestones, organizations ensure that the original information needed for oversight, management, and auditing purposes is not modified or destroyed. Providing an effective method of tracking changes to information over time through strict configuration management and control procedures (including version control) is necessary to: (i) achieve transparency in the information security activities of the organization; (ii) obtain individual accountability for security-related actions; and (iii) better understand emerging trends in the organization's information security program.]

3.6.4 Security Status Reporting

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy during the system Operation/Maintenance lifecycle phase.**

Replace the text within the brackets [].

[*Supplemental Guidance: The results of monitoring activities are recorded and reported on an ongoing basis in accordance with the monitoring strategy. Security status reporting can be: (i) event-driven (e.g., when the information system or its environment of operation changes or the system is compromised or breached); (ii) time-driven (e.g., weekly, monthly, quarterly); or (iii) both (event- and time-driven). Security status reports provide essential information with regard to the security state of the information system including the effectiveness of deployed security controls. Security status reports describe the ongoing monitoring activities employed by the information system owner or common control provider. Security status reports also address vulnerabilities in the information system and its environment of operation discovered during the security control assessment, security impact analysis, and security control monitoring and how the information system owner or common control provider intends to address those vulnerabilities.*

Organizations have significant latitude and flexibility in the breadth, depth, and formality of security status reports. Security status reports can take whatever form the organization deems most appropriate. At a minimum, security status reports summarize key changes to security plans, security assessment reports, and plans of action and milestones.

The frequency of security status reports is at the discretion of the organization and in accordance with federal and organizational policies. Status reports occur at appropriate intervals to transmit significant security-related information about the information system (including information regarding the ongoing effectiveness of security controls employed within and inherited by the system), but not so frequently as to generate unnecessary work.]

3.6.5 Ongoing Risk Determination and Acceptance

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk remains acceptable.**

Replace the text within the brackets [].

[*Supplemental Guidance: The authorizing official or designated representative reviews the reported security status of the information system (including the effectiveness of deployed security controls) on an ongoing basis, to determine the current risk. The use of automated support tools to capture, organize, quantify, visually display, and maintain security status information promotes the concept of near real-time risk management regarding the overall risk posture of the organization. The use of metrics and dashboards increases an organization's ability to make risk-based decisions by consolidating data from automated tools and providing it to decision makers at different levels within the organization in an easy-to-understand format. The risks being incurred may change over time based on the information provided in the security status reports. Determining how the changing conditions affect the mission or business risks associated with the information system is essential for maintaining adequate security.***]**

3.6.6 Information System Removal and Disposal

The below text with **red font** provides guidance from NIST SP 800-37. **Please read the guidance and describe how <Company Name> applies this guidance to implement an information system disposal strategy, when needed, which executes required actions when a system is removed from service.**

Replace the text within the brackets [].

[*Supplemental Guidance: When a federal information system is removed from operation, a number of risk management-related actions are required. Organizations ensure that all security controls addressing information system removal and disposal (e.g., media sanitization, configuration management and control) are implemented. Organizational tracking and management systems (including inventory systems) are updated to indicate the specific information system components that are being removed from service. Security status reports reflect the new status of the information system. Users and application owners hosted on the decommissioned information system are notified as appropriate, and any security control inheritance relationships are reviewed and assessed for impact.***]**

4. Information System Boundaries

4.1 Establishing Information System Boundaries

For CS3 COMSATCOM Task Orders, the Government will identify the information assurance (IA) system boundaries the Offeror must address in their response to the Task Order RFP. Most Department of Defense (e.g., Defense Information Systems Agency) organizations will require

Offerors to submit a completed IA Checklist that provides a complete description and security assessment for the Offeror Task Order IA boundary.

Please describe the processes and resources the <Company Name> employs to develop and maintain documentation on COMSATCOM IA controls for the organization's organic systems and services as well as for services contracted for (e.g., Teleport, space segment).

Note: For most CS3 COMSATCOM services delivered to the Government, the Offeror's IA boundary is where the Offeror's services connect to the user terminals/equipment (i.e., includes satellite command encryption (ground and space); systems used in the Satellite Operations Centers (SOCs), Network Operations Centers (NOCs), and teleport).

Figure 4-1 illustrates the COMSATCOM System Boundaries for the CS3 Sample Task Order #1 (includes the Satellites, Ground Stations, Satellite Operations Center, Network Operations Center and Operations/Business Support Systems and User Terminals). Because the Offeror was required to provide the user terminals (including the LNB/BUC, Modem, Router, Laptop, and VOIP phones), these additional components were also included in the System Boundary.

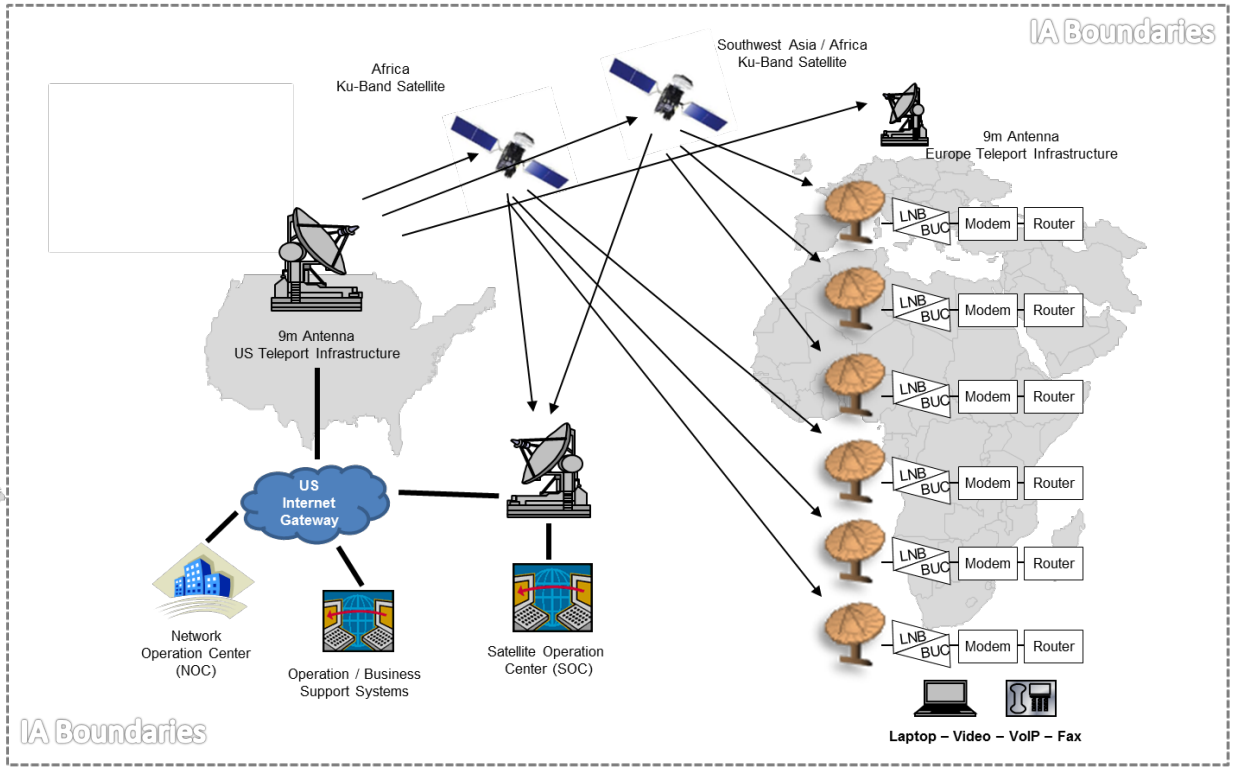

Figure 4-1. CS3 STO-1 COMSATCOM IA System Boundary

Note: The IA System Boundary in Figure 4-1 is greater than a typical COMSATCOM Task Order, where the Offeror's IA System Boundary would end at the user receive satellite terminal as illustrated in Figure 4-2.

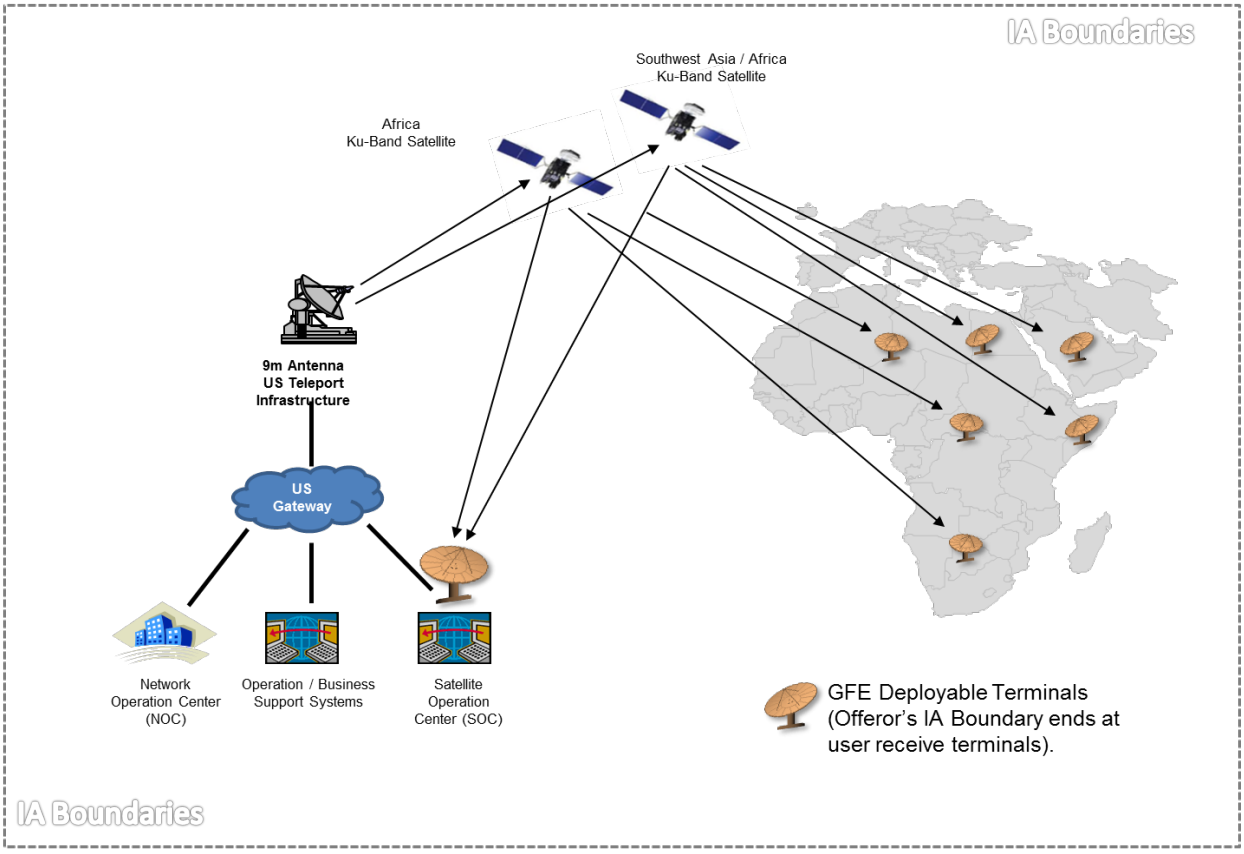

Figure 4-2. Notional CS3 COMSATCOM IA System Boundary

4.2 Changing Technologies and the Effect on Information System Boundaries

Satellite technologies and services are rapidly evolving. Accordingly, the Government anticipates that services and solutions available under CS3 will be increased, enhanced, and upgraded as these improvements become available to COMSATCOM customers. It is anticipated that over the ten year life of the CS3 contracts, the current information assurance policies and procedures for COMSATCOM Complex Solutions will continue to evolve to address system vulnerabilities and cyber-threats. **Describe how <Company Name> will assess the effect new technologies will have on the information system boundaries and what process and procedures are or will be implemented to ensure the Risk Management Framework will be applied for new technologies.**

Appendix A: Information Assurance (IA) Checklist Template

FCSA IA Checklist for
Non-Federal CUI Syst

Appendix B: Security Plan Table of Contents

Appendix C: References

CNSS Instruction No. 1253 *Security Categorization and Control Selection for National Security Systems*
http://www.dss.mil/documents/CNSSI_No1253.pdf

CNSSP No. 12 *National Information Assurance Policy for Space Systems Used to Support National Security Missions*
http://niatec.info/ViewPage.aspx?id=244

FIPS 140-2 *Security Requirements for Cryptographic Modules*
http://csrc.nist.gov/groups/STM/cmvp/standards.html

FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*
https://doi.org/10.6028/NIST.FIPS.199

FIPS 200 Minimum Security Requirements for Federal Information and Information Systems
https://doi.org/10.6028/NIST.FIPS.200

NIST Special Publications 800-30 *Guide for Conducting Risk Assessments*
http://csrc.nist.gov/publications/PubsSPs.html#SP 800

NIST Special Publication 800-37 Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems (A Security Life Cycle Approach)
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

NIST Special Publications 800-39 *Managing Information Security Risk Organization, Mission, and Information System View*
http://csrc.nist.gov/publications/PubsSPs.html#SP 800

NIST Special Publication 800-53 Revision 4 *Security and Privacy Controls for Federal Information Systems and Organizations*
http://csrc.nist.gov/publications/PubsSPs.html#SP 800

NIST Special Publications 800-59 *Guideline for Identifying an Information System as a National Security System*
http://csrc.nist.gov/publications/PubsSPs.html#SP 800

NIST Special Publications 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
http://csrc.nist.gov/publications/PubsSPs.html#SP 800

NIST Special Publication 800-171 *Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations*
http://csrc.nist.gov/publications/PubsSPs.html#SP 800

Appendix D: Glossary

Note: Definitions from NIST 800-37 provided for clarification during development of RMFP

Authorizing Official	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Availability	Ensuring timely and reliable access to and use of information.
Common Control	A security control that is inherited by one or more organizational information systems. See Security Control Inheritance.
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST SP 800-53, that provide equivalent or comparable protection for an information system.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Continuous Monitoring	Maintaining ongoing awareness to support organizational risk decisions.
Controlled Interface	A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Cross Domain Solution	A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.
Environment of Operation	The physical surroundings in which an information system processes, stores, and transmits information.

External Information System (or Component)	An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
Hybrid Security Control	A security control that is implemented in an information system in part as a common control and in part as a system-specific control.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Moderate-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate, and no security objective is assigned a FIPS 199 potential impact value of high.
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

Risk Management	The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Control Inheritance	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Appendix E: Acronyms

NOTE: Add additional acronyms (if required)

A&A	Assessment and Authorization
CNSS	Committee on National Security Systems
COMSATCOM	Commercial Satellite Communications
CS3	Complex Commercial SATCOM Solutions
FIPS	Federal Information Processing Standards Publication
GSA	General Services Administration
IA	Information Assurance
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework
RMFP	Risk Management Framework Plan
SDLC	System Development Life Cycle