SECURITY ASSESSMENT AND

INFORMATION SYSTEM SECURITY ASSESSMENT AND AUTHORIZATION PROCESS

CHAPTER 02

HANDBOOK	ITS-HBK-2810.02-02
EFFECTIVE DATE:	20150201
EXPIRATION DATE:	20180201
RESPONSIBLE OFFICE:	OCIO/ DEPUTY CIO FOR INFORMATION TECHNOLOGY SECURITY

Distribution:

NODIS

Approved

Howard Whyte

5 FEB 2015
Date

(Acting) Senior Agency Information Security Officer

Change History

Version	Date	Change Description	Updated By
1.0		Initial Version	
1.1		Process refinement, grammatical	
1.2		Alignment with HANDBOOK 0031	
1.3	4/6/06	Process refinement, ready for final review	
1.4	4/12/06	Updates per CAO telecom	
1.5	5/24/06	Revised based on comments from ITSM's and CIO's	
1.6	6/13/06	Formatting	
2.0 (B)	1/31/07	Process adjustments and formatting	
2.1 (C)	3/1/08	Process adjustments and formatting	
2.2 (C)	4/1/08	Edit for structure and formatting	
2.3 (C)	4/9/08	Process adjustment and formatting	
2.4 (C)	6/17/08	Process adjustment	
2.5	11/10/10	Update name, number, and format. System replaced with Information System as appropriate. IT replaced with Information System. Added reference to NPR 2810.1. C&A modified to read Security Assessment and Authorization.	
2.6	10/24/12	Extension as updated process is outlined and finalized.	
2.7	10/22/13	Extended for 1 year.	
3.0 (D)	11/14/2014	Updated to align with NASA's risk management framework in accordance with ongoing initial authorization; Updated to consolidate the following ITS-HBKs: 1. ITS-HBK 2810.02-03: FIPS 199 Low Systems 2. ITS-HBK-2810.02-07: Information SSP Numbering Schema	
3.1 (D)		Updated to align with ongoing authorization, define internal and external systems, and the relevant supporting processes.	

Table of Contents

Overview

The Federal Information Security Management Act (FISMA) requires government agencies to ensure information security is implemented in information systems to an acceptable level of risk. The National Institute of Standards and Technology (NIST) developed a methodology called the Risk Management Framework (RMF) to provide government agencies guidance to ensure the appropriate security controls are implemented, assessed and monitored to identify and manage risks associated with operating information systems.

The White House, through the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS), has established government-wide performance measures for federal agency cybersecurity programs.

Security authorization is the official management decision to authorize the operation of an information system and to explicitly accept the risk to operations, assets, or individuals based on the implementation of an appropriate set of security controls. By assessing an information system through issuance of an authorization to operate (ATO), an evaluated level of risk is accepted by NASA senior executives, or Authorizing Officials (AO), for the security posture of their information system and for any adverse impacts should a security breach occur.

Security Assessment & Authorization (SA&A) is part of the risk management process and is an integral part of NASA's information security program. By authorizing a specific system, the AO accepts responsibility for the security of the system and is fully accountable for any adverse impacts to NASA if a breach of security occurs. Responsibility and accountability are core principles that characterize security authorization. Therefore, it is essential that an information system's AO has sufficient factual information regarding the security posture of their system so as to make the appropriate risk based decision on whether to authorize or deny the operation of the system.

All NASA users who are responsible for maintenance and operation of NASA systems, shall be familiar with Information Technology (IT) security, and shall be aware of any IT security assessments required of information systems and the data within their system(s). This handbook augments the National Institute of Standards and Technology (NIST) guidance by providing the reader with NASA-specific requirements, procedures, and recommendations. NASA-specific guidance does not negate NIST guidance, unless explicitly stated. NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology, and the collection of Information Technology Security Handbooks (ITS-HBK) address the fundamental policy and procedural objectives of *NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations*.

1. Introduction

This IT Security Handbook addresses the NASA Agency-wide processes, procedures and standards for implementation of the NIST Risk Management Framework to support the initial security authorization, and reauthorization of internal information systems, also called NASA systems or NASA information systems. While NASA's security responsibilities include all "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source,"[1] the roles, responsibilities, and processes for undergoing an initial security authorization for an internal NASA system are outlined within this publication. The roles, responsibilities, and processes for undergoing security assessment and authorization of external information systems[2] managed and provided by outside agencies, contractors, universities, or other organizations is addressed in ITS-HBK 2810.02-05, *Security Assessment and Authorization: External Information Systems*.[3]

Emerging technologies, combined with threats, which are increasing in both number and sophistication, make it of paramount importance to protect NASA's information via a sound security risk management framework. Human threats may be external (from hackers, spies, terrorists, or professional criminals) or internal (from employees, whether accidental or malicious). Natural threats (floods, earthquakes, electrical storms, etc.) and environmental threats (long-term power failure, pollution, chemicals, etc.) also threaten information. A security risk management framework allows the Agency to prioritize and identify its critical assets, the associated threats, and strategies for mitigating risk using a consistent approach. The objectives of this handbook are to build on existing and planned IT security best practices, and provide a risk management methodology to improve the management of IT security safeguards and mitigation of risks to NASA systems.

Security Authorization applies to all NASA Centers and Mission Directorates and organizations conducting agency business, operating NASA information systems, and collecting and /or maintaining information for, or on behalf of NASA. Primary roles, responsibilities, and processes for undergoing an initial security authorization for NASA systems are outlined within this publication.[4]

[1] FISMA Section 3544(b)

[2] Refer to page 12 of this handbook for a definition of "external information systems"

[3] FISMA requires agencies to apply the RMF to all "information systems used or operated by an agency or by a contractor of an agency or organization on behalf of an agency" in order to provide security protections "…commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency."

[4] While nothing in this handbook precludes implementation of this handbook by system owners and authorizing officials for information systems owned, operated and managed by external system providers, it is acknowledged that many of the roles, responsibilities, and processes may not be applicable.

Once NASA systems have undergone initial authorization, ongoing secure operation is assured by following the criteria outlined in ITS-HBK-2810.02-04: *Continuous Monitoring: Security Control Assessments and Ongoing Authorization*.[5]

Applicable Documents

- *Appendix III to OMB A-130, Security of Federal Automated Information Resources*
- *OMB Circular A-130, Management of Federal Information Resources*
- *OMB Memorandum M-12-20, Fiscal Year (FY) 2012 Reporting Instructions for the FISMA and Agency Privacy Management, September 27, 2012*
- *NIST SP 800-30, Guide for Conducting Risk Assessments*
- *NIST SP 800-37, Guide for Applying the Risks Management Framework to Federal Information Systems*
- *NIST SP 800-39, Managing Information Security Risk*
- *NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations*
- *NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations*
- *NIST SP 800-60 Volume I, Guide for Mapping Types of Information and Information Systems to Security Categories*
- *NIST SP 800-60 Volume II, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*
- *NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security*
- *NIST SP 800-115, Technical Guide to Information Security Testing and Assessment*
- *NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations*
- *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*
- *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
- *NPR 2810.1A, Security of Information Technology*
- *NPR, 1382.1, NASA Privacy Procedural Requirements*
- *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
- *ITS-HBK-1382.03-01, Privacy Risk Management and Compliance: Collections, PIAs and SORNs*
- *ITS-HBK-2810.02-01, Security Assessment and Authorization: Controls*
- *ITS-HBK-2810.02-05, Security Assessment and Authorization: External Information Systems*
- *ITS-HBK -2810.02-04, Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments*
- *ITS-HBK-2810.02-08, Security Assessment and Authorization: Plan of Action and Milestones*

[5] Roles, responsibilities, and processes in ITS-HBK-2810.02-04: *Continuous Monitoring: Security Control Assessments and Ongoing Authorization* may not be applicable for information systems owned, operated, and managed by outside agencies, contractors, universities, or other organizations. Therefore, additional clarifying guidance for continuous monitoring of such systems is contained in ITS-HBK 2810.02-05.

- ITS-HBK-2810.04-01, Risk Assessment: Security Categorization, Risk Assessment, Vulnerability Scanning, Expedited Patching, & Organizationally Defined Values
- *ITS-HBK-2810.04-03, Risk Assessment: Procedures for Information System Security Penetration Testing and Rules of Engagement*
- NASA Agency Common Controls System Security Plan (SSP)

Cancellation

- *ITS-HBK-2810.02-07, Security Assessment and Authorization: Information System Security Plan Numbering Schema*

2. Roles and Responsibilities[6] [7]

The following roles and associated responsibilities are relevant to the activities of this handbook and are in addition to the roles and responsibilities defined in NIST SP 800-37, Appendix D and NPR 2810, Security of Information Technology as they relate to the authorization and assessment of NASA systems.

The Senior Agency Information Security Officer (SAISO) shall:

- Train and oversee personnel with significant responsibilities for obtaining security authorization.
- Select, implement, and assess NASA-defined Common Controls and those portion(s) of NASA Hybrid controls implemented at the Agency-level and publish the results.
- Provide updates to the NASA Chief Information Officer (CIO), as necessary.
- Ensure all Agency information system security documentation, for information systems not overseen by a Center or Mission Directorate, is uploaded and maintained in the NASA Security Assessment and Authorization Repository (NSAAR).
- Ensure that all Agency information systems obtain a valid ATO prior to operational deployment in the enterprise environment.

The Center CIO or Mission Directorate Associate Administrator shall:

- Ensure that information systems under their purview obtain a valid ATO prior to operational deployment in a production environment.

The Center Chief Information Security Officer (CISO) shall:

- Provide oversight to ensure applicable Center/Mission Directorate common and hybrid controls are selected and implemented by the responsible individual or organization.
- Ensure that Center/Mission Directorate common and hybrid controls are assessed and results published for applicable Center/Mission Directorate information systems.

[6] The terms “shall” and “may” within this handbook are used as defined in ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks.

[7] Roles shall be listed out in the order identified within the overarching roles and responsibilities section in NPR 2810.1A. Roles not identified in 2810.1A are listed based on determination of appropriate hierarchy.

- Ensure all Center/Mission Directorate information system security documentation is uploaded and maintained in NSAAR.
- Inform the Center CIO of operational status, unresolved issues, and necessary SA&A actions of information systems.

The Common Control Provider (CCP) shall:

- Provide security control implementation and assessment results to NASA Center CISO or Mission Directorate Security Representative, as applicable, to ensure results are made available to those Information System Owners (ISO) inheriting controls.

The Information System Security Officer (ISSO) shall:

- Review and validate system security categorizations for information systems under their purview.
- Conduct review of information system readiness for the security control assessment (SCA).
    - Document any variances and recommended measures in the information system Security Control Assessment Artifact Checklist.
- Coordinate necessary independent assessments for information systems under their purview.
    - Facilitate communication between independent assessors and ISOs.
- Review the Security Assessment Report (SAR) provided by the Security Control Assessor.
- Ensure the SSP accurately reflects identified findings, and a POA&M has been created for each finding.
- Upload, or input, all security documentation associated with the authorization package into NSAAR.

The Authorizing Official (AO) shall:

- Have adequate knowledge of and training on the related Information Technology Security (ITS) information system requirements outlined within NPR 2810.1A and the ITS handbooks.
- Shall not be any individual directly responsible for implementing or evaluating the system security controls (e.g., Information System Owner (ISO), Information System Security Officer (SSO), or Organizational Computer Security Official (OCSO) to avoid conflict of interest.
- Determine the required level of independence of security control assessments based on the security categorization of information systems and/or the ultimate risk to NASA's mission(s), assets, or individuals.
    - Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the AO receives the most objective information possible in order to make an informed, credible, risk-based, authorization decision.
- Authorize, in writing, and be accountable for the formal signature of ATOs, based on risk acceptance of information systems under their purview.
- Oversee and ensure consistency and compliance, of information systems under their purview, with Federal policies and guidance.

The AO may: Designate and permit the system's AODR to review information system authorization package(s) and system documentation in preparation of formal recommendations and/or guidance on the acceptance of risk. Final approval of an ATO must be signed by the AO.

The Authorizing Official Designated Representative (AODR) shall:

- Review the information system authorization package and associated security documentation.
- Summarize results of security control testing and the overall risk of the information system to the AO prior to the information system obtaining ATO or denial to operate.
- Provide recommendations and/or guidance to AO regarding the acceptance of risk.
- Be allowed to make risk decision recommendations for submission to and approval by the AO.

The Information System Owner (ISO) shall:

- Recommend which NIST security controls are applicable to the information system based on mission/business criticality and security categorization.
    - Collaborate with the Information Owner (IO) to ensure those information system specific mission/business critical security controls are included.
- Documents the Initial Privacy Threshold Analysis (IPTA), performed by the Information Owner, for information systems under their purview.
- Complete the information system Security Control Assessment Artifact Checklist.
- Perform a security categorization of information systems under their purview.
- Assemble the security authorization package for submittal to the AO.
- Develop the strategy for continuous monitoring of the information system, reference ITS-HBK-2810.02-04.
- Complete an IPTA in Privacy & CUI Assessment Tool (PCAT), and if necessary, Privacy Impact Assessment (PIA) in accordance with NPR 1382.1: NASA Privacy Procedural Requirements and ITS-HBK-1382.03-01: Privacy Risk Management and Compliance: Collections, PIAs and SORNs.

The Information Owner (IO) shall:

- Collaborate with the ISO to select information system specific security controls and mission/business critical security controls to be included as part of the security control baseline.
- Develop a Rules of Behavior (ROB) specific to the protection of data within the information system.
- Perform an Initial Privacy Threshold Analysis (IPTA) for information systems under their purview.

The NSAAR Program Manager shall:

- Manage the NSAAR solution and provide guidance to all Centers and Mission Directorates.

- Implement and manage NASA's SA&A program through direct coordination with the Office of the Chief Information Officer (OCIO) Information Technology (IT) Security Division (ITSD) Governance, Risk, and Compliance (GR&C) service executive.
    - Directly or indirectly resolve SA&A related issues and concerns as brought forth from various points throughout the process.
- Facilitate the development and management of the Agency SA&A web site/portal hosted on behalf of OCIO ITSD.

The SA&A Team shall:

- Provide support to the ISO during the execution of assessment responsibilities including:
    - Completion of the SCA Artifact Checklist;
    - Assessment of the implementation of NIST SP 800-53 security controls; and
    - Uploading sufficient evidence as supporting documentation to NSAAR.

The Security Control Assessor (SCA) shall:

- Provide an assessment of the severity of deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address the identified vulnerabilities.
- Conduct a wide-ranging assessment of the management, operational, and technical security controls employed within an information system to determine the effectiveness of the controls.
- Develop a plan to assess the security controls in accordance with NIST SP 800-53A and NIST SP 800-115. Will obtain approval of the plan prior to assessment.

3. Security Assessment and Authorization Process

The Risk Management Framework (RMF) is a collection of guidance documents organized into a framework. NIST developed the RMF to provide a more flexible, dynamic approach for effective management of information systems-related security risk in a highly diverse governmental environment and throughout the system development life cycle. Through implementation of the NIST RMF across NASA, NASA personnel responsible for determining acceptable levels of risk are provided the critical information necessary to make a near real-time risk-based decision.

The six RMF steps include:

1. Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis as low, moderate, or high.

2. 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.

3. Implement the security controls and describe how the controls are employed within the information system and its environment of operation.

4. Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and meeting the security requirements as described in the system security plan.

5. Authorize information system operation based on a determination of the risk resulting from the operation of the information system, and the decision that this risk is acceptable.

6. Monitor the security controls in the information system on an ongoing basis, including assessing control effectiveness, documenting changes to the system (or its operating environment), conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Ongoing authorization is part of RMF Step 5, the Authorize step, and is dependent on the NASA Information Security Continuous Monitoring (ISCM) strategy and program. Information systems maintaining operations and which undergo minor development or configuration changes are required to follow requirements for ongoing authorization. New NASA information systems, or those undergoing significant changes, are required to follow the entire SA&A process.

Security authorization is the process by which a senior management official, the authorizing official (AO), reviews security-related information describing the current security posture of an information system and explicitly accepts or rejects the security risks of operating the system after balancing security risk with mission/business need.

The NASA Security Assessment and Authorization Repository (NSAAR) solution is the official repository for all Security Assessment and Authorization (SA&A) documentation. The process described below is designed to provide the high-level activities that must be completed for NASA information systems within the NSAAR solution. Centers may, at their discretion, use additional processes to ensure SA&A documentation is stored in the NSAAR solution.

NASA information systems exist for the sole purpose of supporting NASA's mission or operations. Examples include Government-owned/government-operated (GOGO) and government-owned/contractor operated (GOCO) information systems and systems operated and/or managed by a contractor on behalf of the government. These systems are often located on/at NASA owned/leased facilities, use NASA internet protocol (IP) addresses, and/or use NASA domain name service (DNS) entries. However, NASA information systems are not limited to only those information systems residing at a NASA facility. NASA information systems are those for which NASA has direct fiduciary responsibility, direct operating responsibility, and those information systems specified by contractual, grant, or other agreement as being owned by NASA.

NASA external information systems are any information system owned, operated, and managed by outside agencies, contractors, universities, or other organizations which store, process, or disseminate

NASA data under a contract or formal agreement with NASA. Security Assessment and Authorization procedures for these systems in context of the RMF are addressed in ITS-HBK.02-05.[8]

The following sections detail NASA's SA&A process for information systems as defined in NPR 2810.1.

3.1. Initial System Security Authorization

Initial authorization is defined as the initial (start-up) risk determination and risk acceptance decision based on a zero-base review of the information system conducted prior to its entering the operations/maintenance phase of the system development life cycle. The zero-base review includes an assessment of *all* security controls (i.e., system-specific, hybrid, and common controls) contained in a security plan and implemented within an information system or the environment in which the system operates.

3.1.1. Responsibilities

With the roles effectively and properly assigned within the Agency and Center/Mission Directorates for all its information systems, the tasks associated with planning, implementing, assessing and mitigating risk, managing and monitoring information security must be performed. NIST, in its special publication for security assessment and authorization (NIST SP 800-37) defines the tasks and assigns the primary responsibility for each task in this process. Also provided is a description of the support provided to the individual or group with the primary responsibility. This information has been augmented with the steps necessary to develop and manage a Cybersecurity Program at the Agency and Center/Mission Directorates levels. Table 1 lists these steps and provides a brief description of each along with the role(s) that have primary and supporting responsibility.

Table 1: Initial System Security Authorization Steps and Associated Responsibility

Step / Task of Initial System Security Authorization	Responsibility	
	Primary	**Support**
Step 1: Categorize the Information System		
***TASK 1-1* Security Categorization** Categorize the information system in accordance with the NIST and document the results of the security categorization in the security plan.	System Owner IO	Risk Executive AO or AODR CIO CISO ISSO
***TASK 1-2* Information System Description**	System Owner	AO or AODR CISO IO

[8] FISMA and OMB policies require that federal agencies using external systems to process, store, or transmit federal information or operate information systems on behalf of the federal government must assure that such use meets the same security requirements that federal agencies are required to meet by incorporating the RMF as part of the terms and conditions in contracts and operation.

Step / Task of Initial System Security Authorization	Responsibility	
	Primary	**Support**
Describe the information system (including system boundary) and document the description in the security plan.		CISO ISSO
TASK 1-3 **Information System Registration** Register the information system in the NASA Security Assessment and Authorization Repository (NSAAR).	CISO	System Owner ISSO
Step 2: Select the Security Controls		
TASK 2-1 **Common Control Identification** Identify the security controls that are provided by the Agency and Center/Mission Directorate as common controls for NASA information systems and document the controls in a security plan (or equivalent document).	CIO or CISO Common Control Provider System Technical Staff	Risk Executive AO or AODR System Owner System Technical Staff
TASK 2-2 **Security Control Selection** Select the security controls for the information system and document the controls in the security plan.	System Owner System Technical Staff	AO or AODR IO ISSO CISO System Technical Staff
TASK 2-3 **Monitoring Strategy** Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes to the information system and its environment of operation. Document this strategy in a Continuous Monitoring Plan.	System Owner or Common Control Provider	Risk Executive AO or AODR CIO CISO IO ISSO
TASK 2-4 **Security Plan Approval** Review and approve the security plan.	AO or AODR	Risk Executive CIO CISO
Step 3: Implement Security Controls		
TASK 3-1 **Security Control Implementation** Implement the security controls specified in the security plan.	System Owner or Common Control Provider	IO ISSO Technical Support Staff
TASK 3-2 **Security Control Documentation** Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation adequate to permit the assessment of its effectiveness.	System Owner or Common Control Provider	IO ISSO Technical Support Staff
Step 4: Assess the Security Controls		
TASK 4-1 **Assessment Preparation** Develop a plan to assess the security controls in accordance with NIST SP 800-53A and NIST SP 800-115. Obtain approval of the plan prior to assessment.	SCA	AODR CIO CISO System Owner

Step / Task of Initial System Security Authorization	Responsibility	
	Primary	Support
		IO ISSO
***TASK 4-2* Security Control Assessment** Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.	SCA	System Owner IO ISSO
***TASK 4-3* Security Assessment Report** Prepare the security assessment report in accordance with NIST SP 800-37 and NIST SP 800-53A documenting the issues and findings. Calculate the risks associated with the findings in accordance with NIST SP 800-30 documenting the results in the Security Assessment Report. Provide recommendations for risk acceptance and remediation.	SCA	System Owner or Common Control Provider ISSO
***TASK 4-4* Remediation Actions** Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediation control(s) as appropriate. Revise the Security Assessment Report to reflect validation of remediation actions.	System Owner or Common Control Provider SCA	AO or AODR CIO CISO IO ISSO Technical Support Staff
Step 5: Authorize the Information System		
***TASK 5-1* Plan of Action and Milestones** Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken. Follow guidance provided in the NASA Plan of Action and Milestones Handbook (*ITS-HBK 2810.02-08-A*).	System Owner or Common Control Provider	IO ISSO
***TASK 5-2* Security Authorization Package** Assemble the security authorization package and submit the package to the Authorizing Official for adjudication.	System Owner or Common Control Provider	ISSO SCA
***TASK 5-3* Risk Determination** Determine the risk to NASA and/or Component operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.	AO or AODR	Risk Executive CISO
***TASK 5-4* Risk Acceptance** Determine if the risk to NASA and/or Center/Mission Directorate operations, organizational assets, individuals, other organizations, or the Nation is acceptable. Issue authorization decision (approval or denial).	AO	Risk Executive AODR CISO
***TASK 5-5* Record Results of Authorization** Report the results of the AO authorization decision along with supporting security authorization documentation	ISSO	CISO

3.1.2. Process and Procedures

The NASA security authorization process is an integral part of overall Risk Management. Managing the risk associated with information systems (including technology and the people, processes, and environment surrounding the technology) is one part of that overall protection. The RMF emphasizes building information security into the culture and infrastructure of an organization. The Initial Security Authorization of a system involves a number of security activities under steps 1-5 of the RMF.

3.1.2.1. Categorize Information Systems

Center/Mission Directorate personnel must follow the process, procedure and associated templates specified in accordance with FIPS Publication 199, NIST SP 800-60 and NASA policy. Categorization of information systems include the security impact level (FIPS PUB 199) but also additional categorization and inventory information required by other federal guidance such as:

- Have goals and business objectives been identified?
- Has an inventory of critical services and assets been completed?
- Has a set of security requirements been developed?
- Is the system a system or subsystem?
- Does the system contain personally identifiable information (PII)?
- Is the system subject to cloud computing requirements?
- Does the system meet the NIST definition of a cloud computing solution?
- What is the current operational state of the system?

Note: If the information system is categorized as a cloud computing solution, the System Owner must comply with guidance published and managed by the GSA FedRAMP Program[9] Office as well as the NASA Computing Services Service Office (CSSO) unless other guidance is in place. The System Owner must integrate the FedRAMP and CSSO guidance into the overall NASA security authorization and continuous monitoring process and procedures specified in this handbook.

During the process of categorizing the information system, critical information regarding the information system must be obtained to support the categorization analysis and inventory of the system. A description of the system including a depiction of the security authorization boundary is critical at this stage. Refer to NIST SP 800-37 for guidance regarding security boundary determinations. The information that describes or depicts the system and its security authorization must be captured in the System Security Plan.

In executing this process, the following key determinations must be made and documented:

a) Does the system store and/or process federal information in support of a federal organization?

[9] http://www.fedramp.gov

b) Does the information system meet the criteria to be classified as either a system or subsystem?

Center/Mission Directorate personnel must follow NIST SP 800-37 and NIST SP 800-53 guidance to determine adequate protection of the information system or application. The result of this analysis must be documented in the System Security Plan of the information system providing the authorization and security control protections.

3.1.2.2. Select Security Controls

The process and procedure for selection and documentation of security controls is described in NIST SP 800-53. Center/Mission Directorate personnel are to follow 800-53 guidance supplemented by the process and procedures specified here to select and document the security controls applicable to the information system. The security control baseline is provided by NIST SP 800-53, based on the FIPS 199 category of the system.

To select security controls, Center/Mission Directorate personnel must:

1. Select all the security controls defined for the information system based on the FIPS PUB 199 Security Impact Level (High, Moderate, or Low), established during the security categorization process. This is referred to as the initial baseline of controls.

2. Tailor the initial baseline security controls by applying scoping, parameterization, and compensating control guidance. Refer to NIST SP 800-53 for guidance on permitted tailoring and scoping. The NASA Common Controls System Security Plan contains parameters for all instances where NIST provides [organizationally-defined] parameters within the security control. In some instances, NASA has required Centers/Mission Directorates to specify some of these parameters. Centers/Mission Directorates personnel must obtain Center-defined security control parameters from the Center CISO. In no instance can Center-defined parameters be less stringent than Agency level parameters.

3. Supplement the tailored and scoped NIST SP800-53 baseline security controls with Agency supplemental security controls for these selected controls.

4. Document the results of control scoping, parameters, compensating controls and applicable Agency supplemental controls in the System Security Plan for each control that is applicable to the system (this includes common, hybrid/shared and system specific controls).

5. Specify the minimum control requirements, as appropriate in accordance with NIST SP 800-53 for the applicable NIST SP 800-53 controls.

6. Using this scoped and tailored baseline of security controls, identify from this set which of the security controls are deemed “common controls” by the Center and or Agency. Confirm the information system can leverage these common controls via the Center CISO or Common Control Provider. Document the common controls along with the owner of the common control (organization and information system) in the System Security Plan.

7. Identify other security controls or portions of security controls that are controlled by another organization (either internal to NASA or external) and document whether the control is fully inherited from these parties or partially inherited where a portion of the control must be

implemented by the Center/Mission Directorate System Owner. These controls are referred to as Hybrid controls. Document these controls and associated owners in the System Security Plan.

The NASA Common Controls SSP provides guidance regarding applicability of security controls through the "Implementation Responsibility" fields provided for all security controls. This column indicates whether the control is applicable at the Agency, Center and/or System Level. Some controls are applicable at all levels. Center personnel are to consult with the Center CISO for guidance regarding definition of and availability of Agency and Center Level common controls.

At this stage, the System Owners must develop the strategy for continuous monitoring of the information system. The strategy should include the monitoring criteria such as the volatility of specific security controls and the appropriate frequency of monitoring specific controls. Refer to the ITS-HBK-2810.02-04A for Agency guidance on monitoring criteria, frequency and security control selection method for continuous monitoring. The monitoring strategy is to be included as an Appendix to the System Security Plan.

The final task of this step is to obtain the approval of the System Security Plan by the Authorizing Official or his/her designated representative (AODR). This approval must be documented (electronic signature or wet signature of the plan) and then uploaded to the NSAAR system.

3.1.2.3. Implement Security Controls

With the security control baseline defined, control type and ownership established, Center/Mission Directorate personnel must determine and document how the information system implements these security controls. Centers/Mission Directorates must 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, Centers /Mission Directorates ensure that mandatory Federal, NASA and Center defined configuration settings are established and implemented on information technology products in accordance with standards. Information system security engineers, with support from information system security officers, employ a sound security engineering process that captures and refines information security requirements and ensures the integration of those requirements into information technology products and systems through purposeful security design or configuration. When available, Centers consider the use of information technology products that have been tested, evaluated, or validated by approved, independent, third-party assessment facilities (e.g., FIPS-approved testing labs for FIPS 140-2 approved products).

For systems with inherited controls and common controls, the System Owner can either document the control implementation of these controls in System Security Plans or reference the controls contained in the System Security Plans of the common and inherited control providers. For the identified common controls inherited by the information system, information system security engineers with support from Center CISO coordinate with the common control provider to determine the most appropriate way to apply the common controls to the Center /Mission Directorate information systems. For certain management and operational controls, formal integration into information technology products,

services, and systems may not be required. For certain types of operational and/or technical controls, implementation may require additional components, products, or services to enable the information system to utilize the previously selected common controls to the fullest extent. For common controls that do not meet the protection needs of the information systems inheriting the controls or that have unacceptable weaknesses or deficiencies, the system owners identify compensating or supplementary controls to be implemented.

When security controls are provided by external providers (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the System Owner:

- Must define the external services provided to the Center/Mission Directorate in support of the system;
- Describe how the external services are protected in accordance with the security requirements of NASA and the Center/Mission Directorate; and
- Obtain the necessary assurances that the risk to NASA operations and assets, individuals, other organizations, and the Nation arising from the use of the external services is acceptable. For example, obtain evidence of NIST-based security authorization with resulting residual security risks.

The System Owner is responsible for documenting security control implementation with sufficient detail to enable a compliant implementation of the control. Documentation of control implementation for NASA supplemental security controls is to be captured in the NIST SP 800-53 base control to which the NASA supplemental security control is associated. To demonstrate, for the example cited above, the System Security Plan would have security control NASA-AC-8. Included in the security control implementation for NASA-AC-8 would be implementation description for AC-8 as well as NASA supplemental security control NASA-AC-8a.

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.

Centers /Mission Directorates can use the recommended priority code designation associated with each security control in the NIST SP 800-53 baselines to assist in making sequencing decisions for control implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control; a Priority Code 2 (P2) control has a higher priority for implementation than a Priority Code 3 [P3] control). This recommended sequencing prioritization helps ensure that foundational security controls upon which other controls depend are

implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources. The implementation of security controls by sequence priority code does not imply the achievement of any defined level of risk mitigation until all of the security controls in the security plan have been implemented. The priority codes are used only for implementation sequencing, not for making security control selection decisions.

3.1.2.4. Assess Security Controls

The Security Assessment Plan (SAP) provides the objectives for the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures. The assessment plan reflects the type of assessment the organization is conducting (e.g., developmental testing and evaluation, independent verification and validation, assessments supporting security authorizations or reauthorizations, audits, continuous monitoring, assessments subsequent to remediation actions). The SAP is reviewed and approved by Security Controls Assessor to ensure that the plan is consistent with the security objectives of NASA and the Center/Mission Directorate, leverages available tools, employs state-of-the-art practices and 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.

When security controls are provided to the Centers/Mission Directorates by an external provider, the Centers/Mission Directorates ensure that 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 Center/Mission Directorate 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 in the Agency Common Controls SSP.

Refer to NIST SP 800-53A for guidance on performing control assessment, documentation and analysis of results of the assessments. Control assessment and analysis will identify controls deemed as satisfying or not satisfying the control objectives. This in indicated in the SAR as:

- Satisfied (S); or
- Other than satisfied (O).

A finding of **satisfied** indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control has been met producing a fully acceptable result. A finding of **other than satisfied** indicates that for the portion of the security control potential anomalies in the operation or implementation of the control may need to be addressed by the System Owner.

Technical testing/scanning performed on the information system such as vulnerability scanning of the operating systems, network devices, web applications, or databases as well as other testing such as

penetration testing and configuration setting audits / deviations must be analyzed and results mapped to applicable security controls to support determination of controls as satisfied or other than satisfied.

The controls deemed "other than satisfied" must undergo risk assessment in accordance with NIST SP 800-30 to arrive at the risk determination of each weakness taking into account any compensating controls.

The results of the security control assessment, including assessment of risk associated with the weaknesses, vulnerabilities and other findings are documented in the Security Assessment Report (SAR). The SAR is one of three key documents in the security authorization package developed for authorizing officials. The SAR includes:

a) Executive summary of the control assessment findings and associated risks

b) Executive summary of technical testing/scanning with associated summary of vulnerabilities detected with associated severity.

c) 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.

d) Risks associated with controls found not to be effectively implemented.

e) Recommendations for mitigating risks and remediating weaknesses.

The System Owner may elect to remediate some of the identified findings prior to finalizing the SAR. Should this option be exercised, the Security Control Assessor must validate remediation activity performed and issue a revised Security Assessment Report which reflects successful remediation.

3.1.2.5. Authorize Information Systems

With the release of the final SAR, the System Owner or ISO must prepare the Plan of Action and Milestones (POA&M). Refer to the ITS-HBK 2810.02.08-A and OMB Memos[10] for guidance on creating and managing POA&Ms. The Information Technology Security Division (ITSD) may request written documentation and relevant artifacts from the Center/Mission Directorate to support monitoring of progress of remediation actions.

The results of the assessment and draft POA&M are coordinated, as appropriate, with the Center/Mission Directorate CISO, CIO and Risk Executive. The coordination is determined by the manner in which the Center/Mission Directorate has implemented the Risk Executive Function. Depending on the system, coordination may be required with Agency OCIO personnel. These individuals review the risks and provide advice or recommendations to the Authorizing Official. The CISO or ISSO assembles these recommendations into an "Authorization Recommendation Letter".

[10] http://www.whitehouse.gov/omb/memoranda_m02-01 and http://m.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-25.pdf

The System Owner assembles the security authorization package. At a minimum it must contain:

- System Security Plan (with associated appendices);
- Security Assessment Report;
- Plan of Action and Milestones;
- Continuous Monitoring Plan; and
- Authorization Recommendation

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 the Center/Mission Directorate or information system by an external provider, the Center/Mission Directorate ensures that the information needed for authorizing officials to make risk-based decisions, is made available by the provider and included in the security authorization package

The authorizing official or designated representative, in collaboration with the CISO, assesses the information contained in the authorization package, and particularly risk assessment information contained in the SAR regarding the current security state of the system or the common controls inherited by the system. The AO seeks input from the Center/Mission Directorate Risk Executive to obtain information the Risk Executive considers crucial to make the final determination of risk to the Center/Mission Directorate.

The explicit acceptance of risk is the responsibility of the authorizing official and cannot be delegated to other officials within the organization. The authorizing official considers many factors when deciding if the risk to Component 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 Center/Mission Directorate and Agency officials as deemed necessary. 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 Decision Letter conveys the final security authorization decision from the authorizing official to the system owner or common control provider, and other Center/Mission Directorate officials, as appropriate. The authorization decision document contains the following information:

- Authorization decision;
- Terms and conditions for the authorization; and
- Authorization termination date or indication of ongoing authorization subject to continuous monitoring.

The security authorization decision indicates to the information system owner whether the system is:

- Authorized to Operate (ATO); or
- 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 terms and conditions must also specify that ongoing security authorization will be performed through continuous monitoring and that the results of continuous monitoring must be provided to the Authorizing Official at least annually.

The authorization decision document is attached to the security authorization package containing the supporting documentation and transmitted to the system owner or common control provider and the Center/Mission Directorate. Upon receipt of the authorization decision document and original authorization package, the system owner or common control provider acknowledges and implements the terms and conditions of the authorization and notifies the authorizing official.

The Center/Mission Directorate ensures that authorization documents for both information systems and for common controls are made available to appropriate Agency and Center/Mission Directorate officials.

3.1.2.6. Marking of Documentation

All documents and information associated with security planning, assessment and authorization that contain information about the system design/configuration and system vulnerabilities, are to be marked and appropriately protected in accordance with federal and NASA policies.

3.2. Ongoing Authorization

When the RMF has been effectively applied across the organization and the organization has effectively implemented a robust ISCM program, organizational officials, including AOs, are provided with a view of the organizational security and risk posture and each information system's contribution to that security and risk posture on demand. Thus, information systems must move from a static, point-in-time authorization process to a dynamic, near real-time ongoing authorization process.

The following conditions must be met to maintain ongoing authorization:

- Condition 1 – In accordance with the RMF, the information system has been granted an initial authorization to operate by the AO as a result of a complete, zero-base review of the system and has entered the operations/maintenance phase of the system development life cycle.
- Condition 2 – Information System is monitored for all implemented security controls with the appropriate degree of rigor and at the appropriate frequencies specified in the ITS-HBK - 2810.02-04, Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments.

The AO must formally acknowledge that the information system is now being managed by an ongoing authorization process and accepts the responsibility for performing all necessary activities associated with that process. The transition to ongoing authorization must be formally documented by the AO by issuing a new authorization decision document. The security-related information generated through the continuous monitoring process is provided to the AO and other organizational officials in a timely manner through security management and reporting tools.

3.2.1. Reauthorization

Events may occur that trigger the immediate need to assess security controls or verify security status outside of requirements expressed in the Continuous Monitoring strategy. This may require an unplanned assessment. Events such as security incidents, new threat information, significant changes to systems and operating environments, new or additional mission responsibilities, results of a security impact analysis (SIA) or assessment of risk or the change in assignment of the Authorizing Official all may trigger a special assessment. The Authorizing Official will make the final determination as to when reauthorization should occur.

Significant changes to an information system may include for example:

- Installation of a new or upgraded operating system, middleware component, or application;
- Modifications to system ports, protocols, or services;
- Installation of a new or upgraded hardware platform;
- Modifications to cryptographic modules or services; or
- Modifications to security controls.
- A change in the authorizing official;
- An increased number of findings/weaknesses/deficiencies from the CM program;
- A significant change in risk assessment findings;
- Moving to a new facility;
- Adding new core missions or business functions;
- New threat/Vulnerability/impact information; and
- Establishing new/modified laws, directives, policies, or regulations.

If a formal reauthorization action is initiated, the Center/Mission Directorate targets only the specific security controls affected by the changes and reuses previous assessment results wherever possible. Most routine changes to an information system or its environment of operation should be handled in accordance with the NASA handbook ITS-HBK-2810.02-04A.

If the scope or impact cannot be ascertained or the Authorizing Official requires a full reauthorization of the system, the process for completing a reauthorization is:

a) Follow the processes and procedures in Section 3.1 for Initial System Security Authorization.

b) Update existing documents to ensure system information, control selection, control implementation and security authorization boundary are current.

c) Perform a full assessment of all the security controls.

d) Obtain security assessment results from common control providers and for inherited controls.

e) Prepare the Security Assessment Report with the findings and associated assessment of risk.

f) Update the POA&M in accordance with ITS-HBK 2810.02-08 (Security Assessment and Authorization: Plan of Action and Milestones), OMB M-02-01 (Guidance for Preparing and Submitting Security Plans of Action and Milestone), and OMB M-04-25 (FY 2004 Reporting Instructions for the Federal Information Security Management Act (FISMA)).

g) Prepare the Authorization Recommendation.

h) Assemble the Security Authorization package.

i) Brief the Authorizing Official and obtain Authorization to Operate.

Appendix A: NASA's Security Authorization Program Website

NASA's Security Authorization program is governed by a variety of Federal and Agency laws, policies, procedures, standards, and guidelines. A website, under the management of the OCIO, is maintained to support SA&A management across NASA Centers and Mission Directorates.

You are encouraged to visit the SA&A website regularly to keep up-to-date with NASA's SA&A program, policies, procedures, guidance, supporting forms, and NIST documents.

- http://inside.nasa.gov/ocio/content/nasa-welcome-to-nasas-security-authorization-program

If your role with NASA is integral to SA&A procedures and processes, please familiarize yourself with the information and resources provided within this Handbook.

Appendix B: NASA Security Plan Numbering Schema

All information system security plans shall have a unique identifier that consists of multiple fields separated by hyphens: **AA-mmmm-a-bbb-nnnn**

An explanation of each field is:

- **[AA]** - This is a two letter field that identifies the functional office that is responsible for the system security plan. There are currently 23 possible functional offices and sub-offices with AOs that can authorize NASA information systems. Accordingly, this field must have one of the following values[11]:

AR	Aeronautics Research Mission Directorate
CD	Multi-Program systems which support multiple Mission Directorates (authorized by the Center Deputy Director or Center CIO)
ED	Chief Education Officer
EG	Office of the Chief Engineer
ER	External Relations
EX	*Exploration Systems Mission Directorate (now included in HE)*
FO	Office of the Chief Financial Officer
GC	Office of General Counsel
HE	Human Exploration and Operations Mission Directorate
HM	Office of Chief Health and Medical Officer
IE	NASA Enterprise Application Competency Center
IG	Office of Inspector General
IM	Mission Support Directorate
IO	Office of Chief Information Officer
IP	Innovative Partnership Program
OA	Office Automation Information Technology (OAIT)
OS	Office of Security and Program Protection
PA	Office of Program Analysis and Evaluation
PI	Program and Institutional Integration
SC	Science Mission Directorate
SO	*Space Operations Mission Directorate (now included in HE)*
ST	Space Technology Mission Directorate
SP	Office of Safety and Mission Assurance Systems
NN	External (Non-NASA) Systems (Contains/processes NASA information.)[12]

- **[mmmm]** - This is a three digit numeric field used to identify the information system within a Center. Mission Directorate Security Representatives shall leverage guidance from their hosting Center for this code. NOTE: If a Center chooses not to utilize this field for internal organizational identification, this number can default to '9999'.
- **[a]** - This is a single letter field that identifies the FIPS-199 security categorization of the information system:

[11] Values in italics are listed for historical reference purposes and have been consumed by the listed office value
[12] Additional information regarding the SA&A of external information systems is found in ITS-HBK-2810.02-05: *SA&A External Systems*.

L – Indicates the system is Low

M – Indicates the system is Moderate

H – Indicates the system is High

- **[bbb]** - This is a three letter field that identifies the Center that is responsible for tracking the information system. This is usually where the information system is located, managed, or reported. Mission Directorate Security Representatives shall leverage guidance from their hosting Center for this code. There are 12 possible values for this field, as follows:

ARC	Ames Research Center
AGC	Agency
AFR	Armstrong Flight Research Center (formerly Dryden Flight Research Center, DFR)
GRC	Glenn Research Center
GSF	Goddard Space Flight Center
JPL	Jet Propulsion Laboratory
JSC	Johnson Space Center
KSC	Kennedy Space Center
LRC	Langley Research Center
MSF	Marshall Space Flight Center
NHQ	NASA Headquarters
NSS	NASA Shared Services Center
SSC	Stennis Space Center

- **[nnnn]** - This is a four digit numeric field that identifies the information system.

Examples:

OA-1001-L-AFR-1002: This is an example of a valid system security plan number for an OAIT LAN System located at the Armstrong Flight Research Center.

HE-9999-L-KSC-6601: This is an example of a valid system security plan number for a Human Exploration and Space Operations system located at Kennedy Space Center.

Appendix C: SAMPLE Security Control Assessment Artifact Checklist

The checklist below is provided as a SAMPLE security control assessment artifact checklist. NASA Centers and Mission Directorates are encouraged to revise the document as necessary to meet Tier 2 needs.

Information System Name:	**Acronym:**
Center / Mission Directorate:	**Security Plan Number:**
Information System Owner:	**Signature/Date:**
Assessment and Authorization Official:	**Signature/Date:**

Requested Artifact	Control	File Name	Notes/Feedback	L	M	H
01) System Security Plan (SSP)	PL-02			X	X	X
02) SSP Signature Page	CA-06			X	X	X
03) POA&M (Latest)	CA-05			X	X	X
04) SAR (Latest)	CA-02			X	X	X
05) Risk Acceptance Letter (Latest)	RA-03, CA-06			X	X	X
06) Risk Assessment Report (Latest)	RA-03			X	X	X
07) Risk Assessment Report Signature Page	RA-03			X	X	X
08) Scheduled Network "Freezes" (if applicable)	CM-09			X	X	X

Requested Artifact	Control	File Name	Notes/Feedback	L	M	H
09) Hardware Inventory	CM-08			X	X	X
10) Software Inventory	CM-08			X	X	X
11) Configuration Baseline Documentation	CM-02			X	X	X
12) Contingency Plan	CP-02			X	X	X
13) Contingency Plan Signature Page	CP-02			X	X	X
14) Contingency Plan Test Report	CP-04			X	X	X
15) Continuous Monitoring Plan	CA-07			X	X	X
16) Nessus vulnerability Scans within 30 days (last 3 months of scan data)	RA-05			X	X	X
17) Foundstone Vulnerability Scans (last 3 months of scan data)	RA-05			X	X	X
18) Credential Scan within 30 days (if available)	RA-05			X	X	X
19) Ports, Protocols and Services matrix	CM-02			X	X	X
20) Firewall Rules (in text file format)	CM-02			X	X	X
21) Router Configuration (in text file format)	CM-02			X	X	X
22) Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), Memorandum of Agreement (MOA) or Access Agreements	CA-03, SA-09			X	X	X
23) System Rules of Behavior	PL-04			X	X	X

Requested Artifact	Control	File Name	Notes/Feedback	L	M	H
24) Initial Privacy Threshold Analysis (IPTA), Privacy Impact Assessment (PIA)	PL-05			X	X	X
25) Security Impact Analysis Template	CM-04			X	X	X
26) Information System Recovery and Reconstitution Documentation	CP-10			X	X	X
27) Incident Response Plan	IR-08			X	X	X
28) Maintenance Records	MA-02			X	X	X
29) Security Incident Reports (last 12 months)	IR-06			X	X	X
30) Security Assessment Artifact Checklist (this document)	SA-05			X	X	X
31) Configuration Management Plan	CM-09				X	X
32) Change Configuration Board (CCB) Template	CM-03				X	X
33) Developer Configuration Management	SA-10				X	X
34) Developer Security Testing	SA-11				X	X
35) Penetration Test Report within 365 days	RA-05					X

Appendix D: Acronyms

AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authorization To Operate
CCP	Common Control Provider
CIO	Chief Information Officer
CISO	[Center] Chief Information Security Officer
CSSO	Computing Services Service Office
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GOCO	Government-Owned/Contractor-Operated
GOGO	Government-Owned/Government-Operated
GR&C	Governance, Risk, and Compliance
HBK	Handbook
IO	Information Owner
IPTA	Initial Privacy Threshold Assessment
CISSE	Center Information System Security Engineer
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
ITCP	Information Technology Contingency Plan
ITS	Information Technology Security
ITSD	Information Technology Security Division
LOE	Level of Effort
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
NSAAR	NASA Security Assessment and Authorization Repository
OCIO	Office of the Chief Information Officer

OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
POC	Point of Contact
RMF	Risk Management Framework
ROB	Rules of Behavior
SA&A	Security Assessment and Authorization
SAISO	Senior Agency Information Security Officer
SAP	Security Assessment Plan
SAR	Security Assessment Report
SCA	Security Control Assessment
SCAPP	Security Control Assessment Plan and Procedures
SDLC	System Development Life Cycle
SIA	Security Impact Analysis
SORN	System of Records Notice
SP	Special Publication
SSP	System Security Plan
US	United States

Appendix E: Sample Authorization Letter

TO: Information System Owner

FROM: Authorizing Official

SUBJECT: Security Authorization Decision for the [information system name], [information system number]

After reviewing the security authorization package for the [information system name] information system [information system number] and its constituent components, I have determined that the risk to Agency operations, Agency assets, or individuals resulting from the operation of the information system is acceptable. My risk determination is based on the contents of the security authorization package, including the security assessment report and the Plan of Actions and Milestones (POA&M). Accordingly, I am issuing an Authorization to Operate (ATO), valid so long as the conditions enumerated below are met. This security authorization is my formal declaration that adequate security controls have been implemented in the information system, and the residual risk is acceptable to the Agency.

For this authorization to remain valid, you as the Information System Owner (ISO) shall:

a) Conduct continuous testing and review of security controls as required by *ITS-HBK-2810.02-04, Security Assessment and Authorization: Continuous Monitoring*
b) Ensure that all risks, vulnerabilities, or control exceptions (weaknesses) identified during the continuous monitoring process are promptly reported, appropriately mitigated, and do not result in additional Agency-level risk deemed unacceptable by me;
c) Ensure any risks, vulnerabilities, and control exceptions are documented in your Plan of Actions and Milestones (POA&M), including elements from the Security Assessment Report;
d) Ensure significant changes to the information system are reviewed to determine whether re-assessment and re-authorization of the information system are required;
e) Submit monthly status reports to report testing and review of security controls, track POA&Ms entries, ensure risks are managed, and report deviations from the above conditions;
f) Operate the information system in a manner consistent with Federal law, NASA policy, and the conditions of the authorization, including the duration of this authorization.

A copy of this letter with all supporting security assessment and authorization documentation must be retained in accordance with the Agency's record retention schedule.

Authorizing Official

cc:

Appendix F: Sample Authorization with Conditions Letter

TO: Information System Owner

FROM: Authorizing Official

SUBJECT: Security Authorization Decision for the [information system name], [information system number]

After reviewing the security authorization package for the [information system name] information system [information system number] and its constituent components, I have determined that the risk to Agency operations, Agency assets, or individuals resulting from the operation of the information system is acceptable, subject to conditions. My risk determination is based on the contents of the security authorization package, including the security assessment report and the Plan of Actions and Milestones (POA&M). Accordingly, I am issuing an Authorization to Operate (ATO), valid so long as the conditions enumerated below are met. This security authorization is my formal declaration that appropriate security controls have been implemented in the information system, and the residual risk is acceptable to the Agency.

For this authorization to remain valid, you as the Information System Owner (ISO) shall:

a) Within 30 days, update the security plan to fully address [specific controls to be addressed in 30 days], specifically:
b) Submit, within 90 days for review, a written plan to comprehensively address issues related to [specific controls to be addressed in 90 days], specifically:
    i. [Specific actions for controls to be addressed in 90 days], and
    ii. [Additional specific actions for controls to be addressed in 90 days];
c) Within one year, develop a detailed analysis of [information system] [specific controls to be addressed in 1 year], specifically:
    i. [Specific actions for controls to be addressed in 1 year], and
    ii. [Additional specific actions for controls to be addressed in 90 days];
d) Conduct continuous testing and review of security controls as required by *ITS-HBK-2810.02-04, Security Assessment and Authorization: Continuous Monitoring*
e) Ensure that all risks, vulnerabilities, or control exceptions (weaknesses) identified during the continuous monitoring process are promptly reported, appropriately mitigated, and do not result in additional Agency-level risk deemed unacceptable by me;
f) Ensure any risks, vulnerabilities, and control exceptions are documented in your Plan of Actions and Milestones (POA&M), including elements from the Security Assessment Report;
g) Ensure significant changes to the information system are reviewed to determine whether re-assessment and re-authorization of the information system are required;
h) Submit monthly status reports to report testing and review of security controls, track POA&Ms entries, ensure risks are managed, and report deviations from the above conditions;
i) Operate the information system in a manner consistent with Federal law, NASA policy, and the conditions of the authorization, including the duration of this authorization.

A copy of this letter with all supporting security assessment and authorization documentation must be retained in accordance with the Agency's record retention schedule.

Authorizing Official

cc:

Appendix G: Sample ATO Recommendation Letter

TO: Authorizing Official

FROM: Authorizing Official Designated Representative (AODR) or Chief Information Security Officer (CISO)

SUBJECT: Security Authorization Decision for the [information system name], [information system number]

This memo documents the <Organization> recommendation to the Authorizing Official for the [information system name] information system [information system number]. As recommended by the security control assessment team, I concur with an Authorization to Operate (ATO), valid so long as the conditions enumerated below are met. In addition, I recommend specific conditions be associated with the ATO as delineated below, and request direction to the Information System Owner (ISO) to explicitly provide status information to my office.

The assessment team performed a full assessment of the information system with an overall Federal Information Processing Standards (FIPS) 199 rating of Moderate. The assessment team assessed a Low risk to the Agency, and recommended an ATO.

I have reviewed the authorization package, and recommend the following conditions be established in the system's ATO.

a) Conduct continuous testing and review of security controls as required by *ITS-HBK-2810.02-04, Security Assessment and Authorization: Continuous Monitoring*
b) Ensure that all risks, vulnerabilities, or control exceptions (weaknesses) identified during the continuous monitoring process are promptly reported, appropriately mitigated, and do not result in additional Agency-level risk deemed unacceptable by me;
c) Ensure any risks, vulnerabilities, and control exceptions are documented in your Plan of Actions and Milestones (POA&M), including elements from the Security Assessment Report;
d) Ensure significant changes to the information system are reviewed to determine whether re-assessment and re-authorization of the information system are required;
e) Submit monthly status reports to report testing and review of security controls, track POA&Ms entries, ensure risks are managed, and report deviations from the above conditions;
f) Operate the information system in a manner consistent with Federal law, NASA policy, and the conditions of the authorization, including the duration of this authorization.

I thank you for considering these suggestions and requests. If there are any questions, please contact me at XXX-XXX-XXXX or <AODR/CISO Email>@nasa.gov. I will continue to coordinate these recommendations with your designated representatives.

AODR or CISO

cc:

Appendix F: Sample ATO Recommendation with Conditions Letter

TO: Authorizing Official

FROM: Chief Information Security Officer (CISO) Authorizing Official Designated Representative (AODR) or Chief Information Security Officer (CISO)

SUBJECT: Security Authorization Decision for the [information system name], [information system number]

This memo documents the <Center> Chief Information Security Officer (CISO) recommendations to the Authorizing Official (AO) for the [information system name] information system [information system number] for a full three-year Authorization to Operate (ATO). I recommend specific conditions be associated with the ATO, and request direction to the Information System Owner (ISO) to provide status information to my office.

The assessment team performed an assessment of the information system with an overall Federal Information Processing Standards (FIPS) 199 rating of High. The assessment team assessed a High risk to the Agency, and recommended a conditional six-month ATO. The ISO is requesting an ATO for the maximum of three years. I have reviewed the authorization package, and recommend the conditions enumerated below be established in the system's ATO. Based on reviewing the team's recommendations, consultation with the [information system] staff and Deputy CISO, and the ISO's responsive actions to the identified issues, I concur with the ISO's request for an ATO for three years.

I recommend the following conditions specific to this information system:

a) Within 30 days, update the security plan to fully address [specific controls to be addressed in 30 days], specifically:
b) Submit, within 90 days for review, a written plan to comprehensively address issues related to [specific controls to be addressed in 90 days], specifically:
    i. [Specific actions for controls to be addressed in 90 days], and
    ii. [Additional specific actions for controls to be addressed in 90 days];
c) Within one year, develop a detailed analysis of [information system] [specific controls to be addressed in 1 year], specifically:
    i. [Specific actions for controls to be addressed in 1 year], and
    ii. [Additional specific actions for controls to be addressed in 90 days];
d) Conduct continuous testing and review of security controls as required by *ITS-HBK-2810.02-04, Security Assessment and Authorization: Continuous Monitoring*
e) Ensure that all risks, vulnerabilities, or control exceptions (weaknesses) identified during the continuous monitoring process are promptly reported, appropriately mitigated, and do not result in additional Agency-level risk deemed unacceptable by me;
f) Ensure any risks, vulnerabilities, and control exceptions are documented in your Plan of Actions and Milestones (POA&M), including elements from the Security Assessment Report;
g) Ensure significant changes to the information system are reviewed to determine whether re-assessment and re-authorization of the information system are required;

h) Submit monthly status reports to report testing and review of security controls, track POA&Ms entries, ensure risks are managed, and report deviations from the above conditions;
i) Operate the information system in a manner consistent with Federal law, NASA policy, and the conditions of the authorization, including the duration of this authorization.

I thank you for considering these suggestions and requests. If there are any questions, please contact me at XXX-XXX-XXXX or <AODR/CISO Email>@nasa.gov. I will continue to coordinate these recommendations with your designated representatives.

AODR or CISO

cc: