IT Security Handbook

Security Assessment and Authorization

ITS-HBK-2810.02-01 -
Effective Date: 20110506 -
Expiration Date: 20130506 -
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

Distribution:

NODIS

Approved

Valarie Burks

Valarie Burks
Deputy Chief Information Officer for
Information Technology Security

May 6, 2011

Date

Change History

Version	Date	Change Description
1.0	5/2/11	Initial Draft

Table of Contents

1 Introduction and Background

1.1 - NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).

1.2 - This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.

1.3 - *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy*, *NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.

1.4 - *NPR 2810.1, Security of Information Technology,* designates this handbook as a guide of NASA's Security Assessment and Authorization (CA) information security controls.

1.5 - 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*.

1.6 - The Security Assessment and Authorization control family relates to the activities and requirements surrounding the routine testing of security controls, the continuous monitoring of system security posture, and the ongoing risk-based decisions to approve or deny the use of a system. Officials within the NASA community are responsible for continuously ensuring the effectiveness of security control implementations throughout the life cycle of a system. Moreover, in light of an ever-changing security landscape, designated NASA officials should always be prepared to determine the impact of a system's operation on the success of the NASA mission.

1.7 - **Applicable Documents**

- *NPD 2810.1, NASA Information Security Policy*
- *NPR 2810.1, Security of Information Technology*
- *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
- *ITS-HBK-2810.02-02, Security Assessment and Authorization: FIPS 199 Moderate & High Systems*
- *ITS-HBK-2810.02-03, Security Assessment and Authorization: FIPS 199 Low Systems*
- *ITS-HBK-2810.02-04, Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments*
- *ITS-HBK-2810.02-05, Security Assessment and Authorization: External Information Systems*
- *ITS-HBK-2810.02-06, Security Assessment and Authorization: Extending an Information System Authorization to Operate Process and Templates*
- *ITS-HBK-2810.02-07, Security Assessment and Authorization: Information System Security Plan Numbering Schema*
- *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*
- *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
- *NIST SP 800-30, Risk Management Guide for Information Technology Systems*
- *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
- *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*

2 Security Assessments (CA-2)

2.1 Roles and Responsibilities

2.1.1 *The Senior Agency Information Security Officer (SAISO) shall*:

2.1.1.1 Ensure the assessment of Agency common controls, and those portions of hybrid controls belonging to the Agency, in a manner consistent with NASA organizationally defined values.

2.1.1.2 Ensure the release of security control assessment details in a manner consistent with NASA organizationally defined values.

2.1.1.3 Establish the level of independence necessary (e.g., independent third-party, self-assessment) in order for security control assessments to satisfy Agency requirements.

2.1.2 *The Authorizing Official (AO) shall*:

2.1.2.1 Approve the methods, procedures, and tools employed to assess security controls in the course of standard assessments and as a part of the continuous monitoring process.

2.1.3 *The Center Chief Information Security Officer (CISO) shall*:

2.1.3.1 Conduct reviews and spot checks of Center information systems throughout the assessment process to ensure security controls are documented and meet the minimum security requirements for the system.

2.1.3.2 Ensure timely reporting on the status of security assessments for information systems at their Center.

2.1.4 *The Organization Computer Security Official (OCSO) shall*:

2.1.4.1 Conduct reviews and spot checks of organizational information systems throughout the assessment process to ensure security controls are documented and meet the minimum security requirements for the system.

2.1.4.2 Ensure timely reporting on the status of security assessments for the information systems within their organization.

2.1.5 *The Information System Owner (ISO) shall*:

2.1.5.1 Ensure the assessment of their systems' security controls in a manner consistent with NASA organizationally defined values.

2.1.5.2 Ensure security documentation (e.g., Security Assessment Report (SAR), System Security Plan (SSP)) is updated in the NASA Security Assessment and Authorization Repository (NSAAR), based on security assessments.

2.1.5.3 Ensure that all methods and procedures used in the assessment of security controls have the concurrence of the AO.

2.1.5.4 Make results from security control assessments available to the AO or a designated representative as a part of the Authorization Package.

3 Information System Connections (CA-3)

3.1 Roles and Responsibilities

3.1.1 *The NASA Chief Information Officer (CIO) shall*:

3.1.1.1 Approve information system interconnections when the involved information system does not have a valid authorization to operate (ATO).

3.1.2 *The AO shall*:

3.1.2.1 Approve information system interconnection agreements when the involved system(s) has a valid ATO, as a part of the approval process for authorization packages.

3.1.3 *The ISO shall*:

3.1.3.1 Ensure a Memorandum of Understanding/Agreement (MOU/A), and Interconnection Security Agreement (ISA), and System Interconnection Implementation Plan (SIIP) is established prior to the interconnection of NASA information systems with external systems.

3.1.3.2 Ensure an ATO is available for external information systems prior to their interconnection with NASA systems.

3.1.3.3 Develop, coordinate, and obtain required approvals for information system interconnections.

3.1.3.4 Ensure each connection between information systems is addressed individually in any related documentation.

3.1.3.5 Ensure that for each information system interconnection details regarding interface characteristics, security requirements, and the nature of the information being shared is documented.

3.1.3.6 Ensure the terms and conditions of interconnection agreements are continuously monitored.

4 Plan of Action and Milestones (CA-5)

4.1 Roles and Responsibilities

4.1.1 *The SAISO shall*:

4.1.1.1 Appoint principal points of contact for Agency-level Plan of Action and Milestones (POA&M) items.

4.1.1.2 Provide oversight of Agency-level POA&M items.

4.1.2 *The Center CISO shall*:

4.1.2.1 Appoint principal points of contact for Center-level POA&M items.

4.1.2.2 Provide oversight of Center-level POA&M items.

4.1.2.3 Ensure timely reporting on the status of POA&M items for information systems at their Center.

4.1.3 *The OCSO shall*:

4.1.3.1 Appoint principal points of contact for POA&M items applicable to their organization.

4.1.3.2 Provide oversight of POA&M items applicable to their organization.

4.1.3.3 Ensure timely reporting on the status of POA&M items for information systems at their organization.

4.1.4 *The ISO shall*:

4.1.4.1 Ensure all POA&M items are traceable to their points of discovery.

4.1.4.2 Ensure POA&M items are documented and updated in NSAAR.

4.1.4.3 Ensure POA&M items detail the following information:

4.1.4.3.1 Descriptions of the observed deficiencies or weaknesses;

4.1.4.3.2 Associated risk level (High, Moderate, or Low);

4.1.4.3.3 The office/organization responsible for the items resolution or remediation;

4.1.4.3.4 Estimated funding/resources required to resolve or remediate the item;

4.1.4.3.5 Key milestones including completion dates and activities towards the resolution or remediation of the item; and

4.1.4.3.6 Changes to key milestones subsequent to their initial documentation (note: milestones should not be deleted or changed directly, rather changes should be documented independently);

4.1.4.4 Report on the status of POA&M items as necessary.

4.1.4.5 Make the details of POA&M items available to the AO or a designated representative as a part of the Authorization Package.

4.1.4.6 Adhere to POA&M item requirements detailed in the Table 1.

4.2 The following table describes specific requirements related to the management of POA&M items for Low, Moderate, and High *FIPS 199* categorized information systems:

Requirement	Low Category	Moderate Category	High Category
All identified unmitigated risks shall be entered as items in the system POA&M item within:	3 Month	1 Month	1 Month

Requirement	Low Category	Moderate Category	High Category
POA&M items should be reviewed by appropriate stakeholders (Center CISO, OCSO, ISO, etc) at least every:	1 Year	6 Months	3 Months
A risk assessment will be conducted for unmitigated vulnerabilities, in accordance with *NIST SP 800-30*, within:	10 Working Days (from identification)	5 Working Days (from identification)	5 Working Days (from identification)
The AO will be advised of all unmitigated risks designated High within:	10 Working Days (from identification)	10 Working Days (from identification)	10 Working Days (from identification)
High risks will be mitigated or accepted by the AO within:	15 Working Days	15 Working Days	15 Working Days
High risks that are unmitigated or not accepted by the AO shall be reported as “POA&M Item Past Due” after:	15 Working Days	15 Working Days	15 Working Days
The AO will be advised of all unmitigated risks designated Moderate or Low within:	30 Working Days	15 Working Days	15 Working Days
Moderate and Low risks that are unmitigated or not accepted by the AO will be reported as “POA&M Item Past Due” after:	6 Months	30 Working Days	30 Working Days
To meet Agency and FISMA reporting requirements, POA&M items are updated by:	The first of each month.	The first of each month	The first of each month.

Table 1 - POA&M Requirements

5 Security Authorization (CA-6)

5.1 **Roles and Responsibilities**

5.1.1 *The AO shall*:

5.1.1.1 Maintain an awareness of the security posture of information systems under their authority.

5.1.1.2 Authorize information systems to operate.

5.1.2 *The Center CISO shall*:

5.1.2.1 Review authorization packages for compliance with all applicable requirements.

5.1.3 *The OCSO shall*:

5.1.3.1 Review authorization packages for compliance with all applicable requirements.

5.1.4 *The ISO shall*:

5.1.4.1 Ensure information systems have been granted an authorization to operate prior to their operation.

5.1.4.2 Ensure information systems are reauthorized in a manner consistent with NASA organizationally defined values.

5.1.4.3 Ensure authorization package documentation is updated in NSAAR, based on security authorizations.

5.1.4.4 Ensure authorization packages contain, at a minimum, the following:

5.1.4.4.1 An authorization letter that includes the time period for which the ATO is effective.

a. The letter may also include specific restrictions, conditions, and/or timelines for the ATO.

5.1.4.4.2 A SSP;

5.1.4.4.3 A SAR; and

5.1.4.4.4 POA&M (as necessary).

6 Continuous Monitoring (CA-7)

6.1 **Roles and Responsibilities**

6.1.1 *The ISO shall*:

6.1.1.1 - Ensure the security posture of information systems is subject to continuous monitoring in a manner consistent with NASA organizationally defined values.

7 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control's enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

800 53 Reference							**FIPS 199 Categorization**		
Family	**#**	**Name**	**Section**	**Parameter**	**Type**	**Description**	**Low**	**Moderate**	**High**
CA	01	Security Assessment and Authorization Policies and Procedures	*Main*	*[1]*	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
CA	02	Security Assessments	*Main*	*[1]*	Frequency	Review of controls for need, and correctness of implementation.	Continuous; As governed by Change Management controls; As required for reauthorization	Continuous; As governed by Change Management controls; As required for reauthorization	Continuous; As governed by Change Management controls; As required for reauthorization
CA	02	Security Assessments	*E 2*	*[1]*	Frequency	Publication of security control assessment details.	1/Year	1/Year	1/Year
CA	02	Security Assessments	*E 2*	*[2]*	Selection	Style of release for security control assessment.	Announced via Memo	Announced via Memo	Announced via Memo
CA	02	Security Assessments	*E 2*	*[3]*	Selection	Organization defined security testing.	Assessment of controls detailed by Memo	Assessment of controls detailed by Memo	Assessment of controls detailed by Memo
CA	05	Plan of Action and Milestones	*Main*	*[1]*	Frequency	Review and update of POA&M items.	By the first of each month.	By the first of each month.	By the first of each month.

800 53 Reference							FIPS 199 Categorization		
Family	**#**	**Name**	**Section**	**Parameter**	**Type**	**Description**	**Low**	**Moderate**	**High**
CA	06	Security Authorization	*Main*	*[1]*	Frequency	Reauthorization of system.	1/3-Years; As governed by Change Management controls	1/3-Years; As governed by Change Management controls	1/3-Years; As governed by Change Management controls
CA	07	Continuous Monitoring	*Main*	*[1]*	Frequency	Report of security posture to appropriate officials and personnel.	1/Year; As governed by Change Management controls	1/Year; As governed by Change Management controls	1/Year; As governed by Change Management controls
CA	07	Continuous Monitoring	*E 2*	*[1]*	Frequency	Planning, scheduling, and execution of specialized security testing/assessments.			
CA	07	Continuous Monitoring	*E 2*	*[2]*	Selection	Testing is announced or unannounced.			
CA	07	Continuous Monitoring	*E 2*	*[3]*	Selection	Type of specialized security testing/assessments.			
CA	07	Continuous Monitoring	*E 2*	*[3][1]*	Reference	Additional types of specialized security testing/assessments.			