



IT Security Handbook

Maintenance -

ITS-HBK- 2810.10-01
Effective Date: 20110506
Expiration Date: 20130506
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

ITS Handbook (ITS-HBK-2810.10-01)
Maintenance

Distribution:

NODIS

Approved

Valarie Burks

Valarie Burks
Deputy Chief Information Officer for
Information Technology Security

4 May 6, 2

Date

Change History

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

Table of Contents

Change History	3 -
1 Introduction and Background	5
2 Controlled Maintenance (MA-2)	6
3 Maintenance Tools (MA-3)	6
4 Non-Local Maintenance (MA-4)	6
5 Maintenance Personnel (MA-5).....	6
6 Timely Maintenance (MA-6)	6
7 Organizationally Defined Values.....	7

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 Maintenance (MA) 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 Maintenance control family relates to the continuous upkeep of information system components. In general, maintenance controls are very system specific, and are typically performed based upon vendor recommendations. Many variable factors are considered when making the appropriate maintenance decisions for a system. The business impact, cost, and likelihood of equipment failure, the cost of the maintenance agreement, and the availability of spare equipment can all influence the application of specific Maintenance controls.
- 1.7 - NASA recognizes that decisions regarding system specific maintenance requirements are best managed at the information system level, where the specific risks are well-understood. However, all Maintenance controls at the information system level must be based on a thorough risk analysis, and accepted risks must be well documented.
- 1.8 - **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*
 - *Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems*
 - *ITS-HBK-0035, Digital Media Sanitization*
 - *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
 - *NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
 - *NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems*
 - *NIST SP 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*
 - *NIST SP 800-100, Information Security Handbook: A Guide to Managers*

2 Controlled Maintenance (MA-2)

2.1 Roles and Responsibilities

2.1.1 *The Information Security Officer (ISO) shall:*

- 2.1.1.1 - Schedule, approve, track, and review maintenance and repair of information system components, in accordance with manufacturer specifications.
- 2.1.1.1.1 This applies to maintenance activities whether performed on-site, off-site, or remotely.
- 2.1.1.1.2 Maintenance records should include:
 - a. - The dates and times of the maintenance activities;
 - b. - The contact information for personnel performing any maintenance activities;
 - c. - Descriptions of the maintenance activities performed;
 - d. - Return Merchandize Authorization (RMA) numbers, shipping addresses, tracking numbers, case numbers, and/or other information related to off-site maintenance; and
 - e. - A list of affected information system components (including equipment control numbers (N-PROP ECN), NASA Equipment Management System (NEMS) numbers, part numbers, model numbers, and/or serial numbers).
- 2.1.1.2 - Notify property custodians of off-site maintenance, or the need to move NASA controlled equipment (with a N-PROP ECN or NEMS tag).
- 2.1.1.3 - Ensure the removal and replacement of N-PROP ECN or NEMS tags prior to delivery of equipment for off-site maintenance, and upon its return.
- 2.1.1.4 - Ensure the sanitization of information system components prior to removal for off-site maintenance activities, in accordance with *ITS-HBK-0035*.
- 2.1.1.5 - Ensure the review of potentially impacted security controls following any maintenance activities.

3 Maintenance Tools (MA-3)

3.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

4 Non-Local Maintenance (MA-4)

4.1 Roles and Responsibilities

4.1.1 *The ISO shall:*

- 4.1.1.1 - Ensure the sanitization of information system components prior to non-local maintenance activities, in accordance with *ITS-HBK-0035*.
- 4.1.1.2 - Ensure adherence to *ITS-HBK-2810.15-01* regarding remote access controls.

5 Maintenance Personnel (MA-5)

5.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

6 Timely Maintenance (MA-6)

6.1 Roles and Responsibilities

6.1.1 *The ISO shall:*

- 6.1.1.1 - Create and maintain a list of security-critical system components for which maintenance support and/or spare parts may be required in a manner consistent with organizationally defined values.
- 6.1.1.2 - Ensure the capability to obtain maintenance support and/or spare parts for security-critical system components within acceptable windows of time in a manner consistent with 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.

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
MA	01	System Maintenance Policy and Procedures	Main	[1]	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
MA	06	Timely Maintenance	Main	[1]	Reference	List of security-critical system components for which maintenance support and/or spare parts may need to be obtained.		ISO defined	ISO defined
MA	06	Timely Maintenance	Main	[2]	Time Period	Window for obtaining maintenance support and/or spare parts for security-critical system components.		72 Hours (Option of 96 Hours if: 1. The moderate-impact categorization is not based on availability; and 2. If the 96-hour timeline is supported by the BIA; and 3. Is approved by the AO.)	24 Hours (Option of 48 Hours if: 1. The high-impact categorization is not based on availability; and 2. If the 48-hour timeline is supported by the BIA; and 3. Is approved by the AO.)