



NASA TECHNICAL HANDBOOK

National Aeronautics and Space Administration

ITS-HBK-2810.10-02 v2024-02

Published: 2024-02-23

**Maintenance
TECHNICAL HANDBOOK**

TABLE OF CONTENTS

Document Properties	3
Document History Log	3
Approval	3
1. Introduction	4
1.1. Purpose	4
1.2. Scope	4
1.3. Point of Contact(s)	5
1.4. Applicability	5
1.5. Applicable Documents	5
1.5.1. Federal Information Processing Standards (FIPS)	5
1.5.2. National Institute of Standards and Technology (NIST)	5
1.5.3. National Aeronautics and Space Administration (NASA)	5
1.5.4. Cancellations, Updates, Consolidations	5
2. Security Controls	5
2.1. Controlled Maintenance (MA-2)	5
2.1.1. Information System Owner (ISO)	6
2.2. Maintenance Tools (MA-3)	6
2.2.1. Senior Agency Information Security Officer (SAISO)	6
2.3. Maintenance Tools Inspect Tools (MA-3(1))	6
2.3.1. Center Chief Information Security Officer (Center CISO)	6
2.4. Maintenance Tools Inspect Media (MA-3(2))	6
2.4.1. Information System Owner (ISO)	6
2.5. Maintenance Tools Prevent Unauthorized Removal (MA-3(3))	7
2.5.1. Center Chief Information Security Officer (Center CISO)	7
2.6. Non-Local Maintenance (MA-4)	7
2.6.1. Information System Owner (ISO)	7
2.7. Non-Local Maintenance Comparable Security/Sanitization (MA-4(3))	7
2.7.1. Information System Owner (ISO)	7
2.8. Maintenance Personnel (MA-5)	7
2.8.1. Information System Owner (ISO)	7
2.9. Maintenance Personnel Individuals without Appropriate Access (MA-5(1))	8
2.9.1. Center Chief Information Security Officer (Center CISO)	8
2.9.2. Information System Owner (ISO)	8
2.10. Timely Maintenance (MA-6)	8
2.10.1. Information System Owner (ISO)	8
Appendix A: Acronyms	8

DOCUMENT PROPERTIES

Document History Log

Document Version	Published Date	Description
1.0	2011-05-02	Initial Draft
1.1	2013-04-30	Extended for 1 year
1.2	2014-04-24	Extended while revision 4 updates are incorporated into the handbook.
1.3	2014-12-04	Extended for updates and revisions
1.4	2015-03-10	Updated Rev 4. Controls and TOC (MA-1)
1.5	2017-02-14	Extended due to updates
1.6	2017-04-13	Updated to reflect new tools and maintain consistency with referenced documents/standards
1.7	2018-08-01	Revised for consistency with new Handbook format
1.8	2019-10-07	Annual Review, fixed formatting issues and added control enhancements selected for baselines.
1.9	2021-09-30	Updated with NIST SP 800-53 Rev. 5 provisions.
2.0	2023-01-31	Annual update.
v2023-06	2023-06-16	Updated to new format
v2024-02	2024-02-23	Annual update

Approval



Associate Chief Information Officer for
Cybersecurity & Privacy

1. INTRODUCTION

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 Rev. 5 Security and Privacy Controls for Information Systems and Organizations, in a manner consistent with the Risk Management Framework (NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy). NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information and Information Systems, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of NIST SP 800-53 Rev.5.

NPR 2810.1 designates this handbook as a guide of NASA's Maintenance (MA) information security controls. This handbook supports implementation of requirements in NPR 2810.1 and NPD 2810.1. It also augments NIST guidance with NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated. The Agency's organizationally defined values are integrated into the control requirements within RSAARCHER in the Risk Information Security Compliance System (RISCS).

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.

1.1. Purpose

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. This Handbook outlines consistent controls for risk analysis and documenting accepted risks.

1.2. Scope

This Handbook applies to maintenance activities for all systems owned and/or operated by NASA.

Although NASA Handbooks may contain "shall" (requirements) statements, they are not intended to be requirements documents. However, pursuant to NPR 1400.1K, portions of NASA Handbooks containing procedural or process guidance may be cited in contract, program, and other Agency documents, and may become requirements when a NASA directive specifies their use by citing the document title, revision letter/number, and date; or, when a NASA manager with authority over a NASA program, project, or other activity, identifies it as a requirement.

This handbook and the procedural guidance contained within remains in full force and effect until such time that the handbook is formally cancelled, rescinded or superseded by an updated document.

A documented rationale and/or justification shall accompany any non-concurrence, disapproval, denial, or request for deviation from the procedural guidance set forth in this handbook to support such decision. The documented rationale/justification shall be provided to the NASA Cybersecurity and Privacy Division (CSPD) and the point of contact for this Handbook, in coordination with Center Information Security Officers (CISO), to review and validate for the record.

1.3. Point of Contact(s)

For any questions or comments regarding the contents of this Handbook, contact:

- hq-dl-cspd-policy@mail.nasa.gov

Any questions or concerns regarding perceived gaps in policy or implementation guidance, conflicting procedural requirements, lack of clarity pertaining to specified roles and responsibilities, or issues associated with interpretation shall be elevated to the NASA CSPD, in coordination with the CISO, and directed to the attention of the point of contact for this particular Handbook to address and resolve.

1.4. Applicability

This Handbook is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to Jet Propulsion Laboratory, a Federally Funded Research and Development Center (FFRDC), other contractors, authorized users, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

1.5. Applicable Documents

1.5.1. Federal Information Processing Standards (FIPS)

- [FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*](#)
- [FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*](#)

1.5.2. National Institute of Standards and Technology (NIST)

- [NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*](#)
- [NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*](#)
- [NIST SP 800-100, *Information Security Handbook: A Guide for Managers*](#)

1.5.3. National Aeronautics and Space Administration (NASA)

- [NPD 2810.1, *NASA Information Security Policy*](#)
- [NPR 2810.1, *Security of Information and Information Systems*](#)
- [ITS-HBK-2810.15-01, *Access Control*](#)
- [ITS-HBK-2810.11-02, *Media Protection and Sanitization*](#)

1.5.4. Cancellations, Updates, Consolidations

- [ITS-HBK-2810.10-01, *Maintenance*](#)

2. SECURITY CONTROLS

2.1. Controlled Maintenance ([MA-2](#))

2.1.1. Information System Owner (ISO)

The ISO:

- Schedules, approves, tracks, and reviews maintenance and repair, and replacement of information system components, in accordance with manufacturer specifications.
 - This applies to maintenance activities whether performed on-site, off-site, or remotely.
- Ensures that maintenance records include:
 - The dates and times of the maintenance activities;
 - The contact information for personnel performing any maintenance activities;
 - Descriptions of the maintenance activities performed;
 - Return Merchandize Authorization (RMA) numbers, shipping addresses, tracking numbers, case numbers, and/or other information related to off- site maintenance; and
 - A list of affected information system components (including NASA property equipment control numbers (N-PROP ECN), NASA Equipment Management System (NEMS) numbers, part numbers, model numbers, and/or serial numbers).
- Notifies property custodians of off-site maintenance, or the need to move NASA- controlled equipment (with a N-PROP ECN or NEMS tag).
- Ensures the removal and replacement of N-PROP ECN or NEMS tags prior to delivery of equipment for off-site maintenance, and upon its return. o Ensures the sanitization of information system components prior to removal for off- site maintenance activities, in accordance with ITS-HBK 2810.11-2C.

2.2. Maintenance Tools (MA-3)

2.2.1. Senior Agency Information Security Officer (SAISO)

The SAISO:

- Approves, reapproves, controls, and monitors information system maintenance tools.

2.3. Maintenance Tools | Inspect Tools (MA-3(1))

2.3.1. Center Chief Information Security Officer (Center CISO)

The Center CISO:

- Ensures inspection of maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

2.4. Maintenance Tools | Inspect Media (MA-3(2))

2.4.1. Information System Owner (ISO)

The ISO:

- Ensures that media containing diagnostic and test programs are checked for malicious code before the media are used in an information system.

2.5. Maintenance Tools | Prevent Unauthorized Removal (MA-3(3))



This control enhancement is selected only for High systems.

2.5.1. Center Chief Information Security Officer (Center CISO)

The Center CISO:

- Coordinates with the Agency Physical Security Chief, as appropriate, to prevent the unauthorized removal of maintenance equipment containing organizational information by:
 - Verifying that there is no organizational information contained on the equipment;
 - Sanitizing or destroying the equipment;
 - Retaining the equipment within the facility; or
 - Obtaining an exemption from the ISO explicitly authorizing removal of the equipment from the facility.

2.6. Non-Local Maintenance (MA-4)

2.6.1. Information System Owner (ISO)

The ISO:

- Ensures the sanitization of information system components prior to non-local maintenance activities, in accordance with ITS-HBK 2810.11-2C.
- Ensures adherence to ITS-HBK 2810.15-01 policy and procedural requirements for remote access controls.
- Documents in the System Security and Privacy Plan (SSP) for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

2.7. Non-Local Maintenance | Comparable Security/Sanitization (MA-4(3))

2.7.1. Information System Owner (ISO)

The ISO:

- Ensures that non-local maintenance and diagnostic services are performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced.
- If the non-local maintenance is not performed from an information system that meets this requirement, ensures that the component being serviced is removed and sanitized of NASA information prior to maintenance, and inspects and sanitizes the component for potentially malicious software before reconnecting the component to the information system.

2.8. Maintenance Personnel (MA-5)

2.8.1. Information System Owner (ISO)

The ISO:

- Establishes a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.
- Ensures that non-escorted personnel performing maintenance on the information system have required access authorization.
- Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

2.9. Maintenance Personnel | Individuals without Appropriate Access (MA-5(1))



This control enhancement is selected only for High systems.

2.9.1. Center Chief Information Security Officer (Center CISO)

The CISO:

- Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
 - Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and
 - Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured.

2.9.2. Information System Owner (ISO)

The ISO:

- Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

2.10. Timely Maintenance (MA-6)

2.10.1. Information System Owner (ISO)

The ISO:

- Creates and maintains a list of security-critical system components for which maintenance support and/or spare parts may be required, in a manner consistent with organization-defined values.
- Ensures 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 organization-defined values.

APPENDIX A: ACRONYMS

CISO	Center Chief Information Security Officer
------	---

CSPD	Cybersecurity and Privacy Division
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards
HBK	Handbook
ISO	Information System Owner
IT	Information Technology
ITS	Information Technology Security
NASA	National Aeronautics and Space Administration
NEMS	NASA Equipment Management System
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
N-PROP ECN	NASA Property Equipment Control Numbers
OCIO	Office of the Chief Information Officer
RISCS	Risk Information Security Compliance System
RMA	Return Merchandize Authorization
SP	Special Publication
SSP	System Security Plan