NASA TECHNICAL HANDBOOK

National Aeronautics and Space Administration

ITS-HBK-2810.14-04 v2024-02

Published: 2024-02-23

System and Information Integrity
TECHNICAL HANDBOOK

TABLE OF CONTENTS

Document Properties . . . 4
Document History Log . . . 4
Approval . . . 4
1. Introduction . . . 5
1.1. Purpose . . . 5
1.2. Scope . . . 5
1.3. Point of Contact(s) . . . 5
1.4. Applicability . . . 6
1.5. Applicable Documents . . . 6
1.5.1. National Institute of Standards and Technology (NIST) . . . 6
1.5.2. National Aeronautics and Space Administration (NASA) . . . 6
1.5.3. Cancellations, Updates, Consolidations . . . 6
2. Roles and Responsibilities . . . 6
2.1. Agency-Wide . . . 6
2.1.1. NASA Senior Agency Information Security Officer (SAISO) . . . 6
2.1.2. Cybersecurity Infrastructure (CSI) Service Owner . . . 7
2.1.3. NASA Consolidated Email Project Manager . . . 7
2.1.4. NASA Security Operations Center (SOC) . . . 8
2.2. Center Level . . . 8
2.2.1. Center Chief Information Security Officer (CISO) . . . 8
2.3. Information System Level . . . 8
2.3.1. Information System Owner (ISO) . . . 8
2.3.2. Information System Security Officer (ISSO) . . . 9
3. Security Controls . . . 9
3.1. System and Information Integrity Policy and Procedures (SI-1) . . . 9
3.1.1. Senior Agency Information Security Officer (SAISO) . . . 9
3.2. Flaw Remediation (SI-2) . . . 9
3.2.1. Senior Agency Information Security Officer (SAISO) . . . 10
3.2.2. CSI Project Manager . . . 10
3.3. Flaw Remediation | Central Management (SI-2(1)) . . . 10
3.3.1. CSI Project Manager . . . 10
3.4. Flaw Remediation | Automated Flaw Remediation Status (SI-2(2)) . . . 10
3.4.1. CSI Project Manager . . . 10
3.5. Malicious Code Protection (SI-3) . . . 10
3.5.1. Senior Agency Information Security Officer (SAISO) . . . 10
3.5.2. Information System Owner (ISO) . . . 10
3.6. Malicious Code Protection | Central Management (SI-3(1)) . . . 11
3.6.1. Security Operations Center (SOC) . . . 11
3.7. Malicious Code Protection | Automatic Updates (SI-3(2)) . . . 11
3.7.1. Security Operations Center (SOC) . . . 11
3.8. Information System Monitoring (SI-4) . . . 11
3.8.1. Senior Agency Information Security Officer (SAISO) . . . 11
3.8.2. Center Chief Information Security Officer (CISO) . . . 11
3.8.3. Information System Owner (ISO) . . . 11
3.8.4. Information System Security Officer (ISSO) . . . 11

3.9. Information System Monitoring | Automated Tools for Real-Time Analysis (SI-4(2)) 12
3.9.1. CSI Project Manager 12
3.10. Information System Monitoring | Inbound and Outbound Communications Traffic (SI-4(4)) 12
3.10.1. Security Operations Center (SOC) 12
3.11. Information System Monitoring | System-Generated Alerts (SI-4(5)) 12
3.11.1. Security Operations Center (SOC) 12
3.12. Security Alerts, Advisories, and Directives (SI-5) 12
3.12.1. SOC Operations Manager 12
3.13. Security Alerts, Advisories, and Directives | Automated Alerts and Advisories (SI-5(1)) 13
3.13.1. SOC Operations Manager 13
3.14. Software and Information Integrity (SI-7) 13
3.14.1. Information System Owner (ISO) 13
3.14.2. Information System Security Officer (ISSO) 13
3.15. Spam Protection (SI-8) 13
3.15.1. Senior Agency Information Security Officer (SAISO) 13
3.15.2. Center Chief Information Security Officer (CISO) 13
3.15.3. Information System Owner (ISO) 14
3.16. Spam Protection | Central Management (SI-8(1)) 14
3.16.1. NASA Consolidated Email Project Manager 14
3.17. Spam Protection | Automatic Updates (SI-8(2)) 14
3.17.1. NASA Consolidated Email Project Manager 14
3.18. Information Input Validation (SI-10) 14
3.18.1. Information System Owner (ISO) 14
3.19. Error Handling (SI-11) 14
3.19.1. Information System Owner (ISO) 14
3.20. Information Handling and Retention (SI-12) 14
3.20.1. Information System Owner (ISO) and Information System Security Officer (ISSO) 15
Appendix A: Acronyms 15

DOCUMENT PROPERTIES

Document History Log

Document Version	Published Date	Description
02A	2017-12-13	Revised to update content and make consistent with new Handbook format
03B	2019-07-24	Made the following updates: • Updated controls to be consistent with SI controls and ODVs in RISCS • Changed the Handbook to be more consistent with the updated format • Minor typographical/grammar/consistency changes
03C	2019-08-06	Annual review. Minor updates. Incorporated input from CISO community received via OATS action.
03D	2021-09-30	Updated with NIST SP 800-53 Rev. 5 provisions.
04D	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 (FIPS 199, *Standards for Security Categorization of 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 SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*). NPD 2810.1, *NASA Information Security Policy*, 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 SP 800-53.

NPR 2810.1 designates this handbook as a guide of NASA's System and Information Integrity (SI) information security controls. The content of this document, in conjunction with NPD/R 2810.1, defines NASA policy and procedures to address SI-1. 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 RSA ARCHER in the Risk Information Security Compliance System (RISCS). The RISCS or RSA ARCHER platform will enable compliance reporting with the security controls with respect to risk management.

1.1. Purpose

This Handbook describes the procedures NASA uses to implement and maintain SI controls in order to ensure that systems and data are not accidentally or maliciously subjected to improper modification.

1.2. Scope

The System and Information Integrity control family relates to the prevention and detection of improper modification or destruction of an information system. The control family also includes ensuring the non-repudiation and authenticity of information, as well as flaw remediation (e.g., patching vulnerable software), malicious code prevention (e.g., anti-virus software), and monitoring of attempts to subvert integrity (e.g., an intrusion detection system).

Although NASA Handbooks may contain "shall" (requirements) statements, they are not intended to be requirements documents. However, pursuant to NPR 1400.1, *NASA Directives and Charters Procedural Requirements*, 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 rational/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. National Institute of Standards and Technology (NIST)

- NIST SP 800-40, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
- NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-83, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
- NIST SP 800-92, *Guide to Computer Security Log Management*

1.5.2. National Aeronautics and Space Administration (NASA)

- NPD 2810.1, *NASA Information Security Policy*
- NASA Information Technology Requirement (NITR) 2800-2, Email Services and Email Forwarding
- NPR 2810.1, *Security of Information and Information Systems*
- ITS-HBK-2810.04-01, *Risk Assessment, Vulnerability Scanning, and Expedited Patching*

1.5.3. Cancellations, Updates, Consolidations

- ITS-HBK-2810.14-01B, System and Information Integrity

2. ROLES AND RESPONSIBILITIES

2.1. Agency-Wide

2.1.1. NASA Senior Agency Information Security Officer (SAISO)

Controls

SI-1, SI-2, SI-3, SI-4, SI-8

NASA Senior Agency Information Security Officer (SAISO):

- Develops, documents, and/or disseminates a system and information integrity policy and implementation procedures.
- Ensures approved ODVs are captured in directives for NASA implementation via updates to NPR 2810.1 and/or appropriate ITS-HBKs.
- Provisions an Agency-wide mechanism for the identification, reporting, and correction of information system flaws.
- Designates patches for critical vulnerabilities of a particularly serious nature that pose a significant threat to the security posture of the Agency as “Expedited.”

2.1.2. Cybersecurity Infrastructure (CSI) Service Owner

Cybersecurity Infrastructure (CSI) Service Owner

- Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation. Installs security-relevant software and firmware updates within the required time period of the release of the updates.
- Ensures that patch management baselines consist of all current vendor critical patches.
- Ensures the patch status of all information system devices on non-guest NASA networks, where possible, are reported in the Continuous Diagnostics and Mitigation (CDM) Enterprise Data Warehouse.
- Determines the patch update schedule.
- Ensures that any devices on NASA networks that continue to exhibit the same unmitigated or unaccepted vulnerabilities identified in three (3) consecutive monthly vulnerability scans are reported to the cognizant Center Chief Information Officer (CIO) and CISO, and addressed with a Plan of Action and Milestones (POA&M) or Risk-Based Decision (RBD) if they don’t already have one.
    - Before notifying, cross-reference in RISCS to review whether the vulnerability has an associated POA&M or RBD.
    - Center CIOs, CISOs, Information System Security Officers (ISSO), or ISOs may choose to disconnect devices with unmitigated vulnerabilities, depending on the severity of the vulnerabilities, or sensitivity of the device.
    - Works with CIO, CISO, ISSO, or ISOs to Operational Technology (OT) that may not be able to support conventional security controls.
- Provides status and metrics of expedited patch deployment.
- Provides data for the Department of Homeland Security (DHS)/CDM dashboard.
- Discovers and report devices situated on the NASA network that do not have the NASA patch management agent installed and that have not been registered by manual inventory.
- Reports to the OCIO monthly any information system devices recorded in the CDM Enterprise Data Warehouse that are not associated with a System Security Plan (SSP).

2.1.3. NASA Consolidated Email Project Manager

Controls

SI-8(1), SI-8(2)

NASA Consolidated Email Project Manager:

- Implements spam protections in the enterprise-wide email service using tools approved by the SAISO.
- Ensures that the enterprise-wide email service automatically updates its built-in spam protection mechanisms.

2.1.4. NASA Security Operations Center (SOC)

Controls

SI-4(4), SI-4(5), SI-5, SI-5(1)

NASA Security Operations Center (SOC):

- Receives information system security alerts and advisories on a regular basis and issues alerts and advisories to appropriate personnel across the Agency.
- Ensures all security directives received from external organizations are evaluated by the OCIO CSPD for applicability to NASA systems and networks.
- Operates, maintains, and monitors Intrusion Detection Systems (IDS) to provide NASA with continuous monitoring capabilities to detect and respond to network intrusions, unusual or unauthorized activities or conditions, or unauthorized access/use of NASA networking resources.
- Manages and operates an Incident Management System (IMS) to collect, report, and update incident information, to include generating and receiving automated alerts. Centrally manages and automatically updates enterprise-wide malicious code protection mechanisms.

2.2. Center Level

2.2.1. Center Chief Information Security Officer (CISO)

Controls

SI-4, SI-8

Center Chief Information Security Officer (CISO):

- Ensures that Center information system monitoring tools are deployed to collect information to track specific types of transactions of interest to the SAISO.
- Ensures the approved organization-defined values (ODVs) implementation are integrated within the Center-level systems and oversees the monitoring process to report alerts, threats, or vulnerabilities to the SOC.
- Manages any Center-specific spam filtering measures used at their Center.

2.3. Information System Level

2.3.1. Information System Owner (ISO)

Controls

SI-2, SI-3, SI-4, SI-7, SI-8, SI-10, SI-11, SI-12, SI-13

Information System Owner (ISO):

- Ensures the remediation or mitigation of all vulnerabilities in accordance with ITS-HBK-2810.04-01, *Risk Assessment, Vulnerability Scanning, and Expedited Patching*.
- Ensures that all information system components are up-to-date with all applicable patches which may impact the security of information as appropriate for the operating environment and accepted risks.
- Ensures the installation of Agency-approved patch management/reporting software agents, and configuration of the software agent to automatically report patch status to CSPD.

- Ensures that all devices are covered by an SSP with a valid Authorization to Operate (ATO).
- Ensures that security controls are properly implemented as documented in RISCS.
- Ensures appropriate actions taken in response to all alerts and advisories that are disseminated by the SOC.
- Provides information to SOC regarding any additional sources of security alert and advisory information that is specific a Center system.
- Implements spam protection for their site and/or system if it does not use the Agency enterprise-wide email service.
- Tailors spam controls for their system if it is an OT system
- Manages and retains information for their systems in accordance with Agency information protection and records management policies.

2.3.2. Information System Security Officer (ISSO)

Controls

SI-3, SI-4, SI-7, SI-12

Information System Security Officer (ISSO):

- Tests information system patches and updates prior to installation, in a manner commensurate with the level of risk.
- Ensures the remediation or mitigation of all vulnerabilities in accordance with ITS-HBK-2810.04-01, *Risk Assessment, Vulnerability Scanning, and Expedited Patching*.
- Ensures that security controls are properly implemented with Agency and Center ODVs where applicable, as documented in RISCS.
- Manages and retains information for their systems in accordance with Agency information protection and records management policies.

3. SECURITY CONTROLS

The controls listed in this Handbook only apply to systems applying a security baseline. In cases where NASA has adopted ODVs for controls or control enhancements for systems with a high baseline, the latter apply.

3.1. System and Information Integrity Policy and Procedures (SI-1)

3.1.1. Senior Agency Information Security Officer (SAISO)

SAISO:

- Develops, documents, and disseminates system and information integrity policy and procedures.
- Ensures approved ODVs are captured in directives for NASA implementation via updates to NPR 2810.1 and/or appropriate ITS-HBKs.
- Ensures consistency of system and information integrity policies and procedures with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

3.2. Flaw Remediation (SI-2)

3.2.1. Senior Agency Information Security Officer (SAISO)

SAISO:

- Develops and deploys an Agency-wide mechanism for the identification, reporting, and correction of flaw remediation.

3.2.2. CSI Project Manager

CSI Project Manager:

- Manages and monitors the information system devices' flaw agents.

3.3. Flaw Remediation | Central Management (SI-2(1))

This control enhancement is part of the High baseline.

3.3.1. CSI Project Manager

CSI Project Manager:

- Manages and monitors the information system devices' flaw agents.

3.4. Flaw Remediation | Automated Flaw Remediation Status (SI-2(2))

3.4.1. CSI Project Manager

CSI Project Manager:

- Employs automated mechanisms on a weekly (or more frequent) basis to determine the state of information system components with regard to flaw remediation.

3.5. Malicious Code Protection (SI-3)

3.5.1. Senior Agency Information Security Officer (SAISO)

SAISO:

- Defines the acceptability of malicious code protection tools for use across the Agency.

3.5.2. Information System Owner (ISO)

ISO:

- Ensures that Agency-approved malicious code protection tools are installed on all information systems under their purview that support the use of malicious code protection tools.
  - Malicious code protection tools should be appropriate for the information systems on which they are installed.
  - Malicious code protection tools should be employed at applicable Agency information system entry and exit points, as well as workstations, servers and/or mobile computing devices on the network.

- Ensures only privileged users are able to make changes to malicious code protection tools, including the ability to skip updates or not scan files automatically.

3.6. Malicious Code Protection | Central Management (SI-3(1))

3.6.1. Security Operations Center (SOC)

SOC:

- Centrally manages malicious code protection mechanisms.

3.7. Malicious Code Protection | Automatic Updates (SI-3(2))

3.7.1. Security Operations Center (SOC)

SOC:

- Automatically updates enterprise-wide malicious code protection mechanisms.

3.8. Information System Monitoring (SI-4)

3.8.1. Senior Agency Information Security Officer (SAISO)

SAISO:

- Defines the acceptability of information system monitoring tools for use across the agency.

3.8.2. Center Chief Information Security Officer (CISO)

Center CISO:

- Ensures that information system monitoring tools are deployed strategically to collect information, and to track specific types of transactions of interest to the Agency, Center, or organization.

3.8.3. Information System Owner (ISO)

ISO:

- Ensures information system monitoring tools and techniques are employed with the objectives of:
  - Detecting information system attacks.
  - Detecting and reporting unauthorized use of information systems.
  - Identifying actions to mitigate the impact of attacks and unauthorized use.
- Ensures the use of automated tools to enable the real-time analysis of events.
- Ensures the association of all information system components with a SSP.

3.8.4. Information System Security Officer (ISSO)

ISSO:

- Ensures the level and intensity of information system monitoring is heightened whenever there are indications of increased risk based on creditable sources of information.
- Ensures that information system inbound and outbound communication is monitored for unusual or unauthorized activities or conditions.
- Reports suspected or actual IT security incidents immediately to the SOC, Center CISO or other appropriate organizations (e.g., Center-specific IT security office, incident response team, or help desk).
- Reports suspected or actual misuse activity, detected in the course of their duties, to the ISO, CISO, SAISO, or other appropriate authority.
- Ensures that information system monitoring tools are deployed strategically to collect information, and to track specific types of transactions of interest to the Agency, Center, or organization.

3.9. Information System Monitoring | Automated Tools for Real-Time Analysis (SI-4(2))

3.9.1. CSI Project Manager

CSI Project Manager:

- Employs automated tools to support near real-time analysis of events.

3.10. Information System Monitoring | Inbound and Outbound Communications Traffic (SI-4(4))

3.10.1. Security Operations Center (SOC)

SOC:

- Operates, maintains, and monitors IDS to provide NASA with continuous monitoring capabilities to detect and respond to network intrusions, or unauthorized access/use of NASA networking resources.

3.11. Information System Monitoring | System-Generated Alerts (SI-4(5))

3.11.1. Security Operations Center (SOC)

SOC:

- Manages and operates an IMS to collect, report, and update incident information, to include generating and receiving automated alerts.

3.12. Security Alerts, Advisories, and Directives (SI-5)

3.12.1. SOC Operations Manager

SOC Operations Manager:

- Ensures the SOC is the primary interface with the United States Computer Emergency Readiness Team (US-CERT) and other outside agencies, and generate and broadcast internal security alerts and advisories as neces-

sary.

- Ensures that security alerts, advisories, and directives from external sources can be received on an ongoing basis.
- Ensures dissemination of information security alerts, advisories, and directives.

3.13. Security Alerts, Advisories, and Directives | Automated Alerts and Advisories (SI-5(1))

This control enhancement is part of the High baseline.

3.13.1. SOC Operations Manager

SOC Operations Manager:

- Ensures the SOC is the primary interface with the United States Computer Emergency Readiness Team and (US-CERT) and other outside agencies, and generate internal security alerts and advisories as necessary.

3.14. Software and Information Integrity (SI-7)

3.14.1. Information System Owner (ISO)

ISO:

- Ensures that the system employs (automated, if at all possible) capabilities that:
  - Detect unauthorized changes to software and information.
  - Notify the appropriate parties when unauthorized changes are detected.
  - Takes relevant action when unauthorized changes are detected.

3.14.2. Information System Security Officer (ISSO)

ISSO:

- Verifies the integrity of software and information through periodic system scans.

3.15. Spam Protection (SI-8)

3.15.1. Senior Agency Information Security Officer (SAISO)

SAISO:

- Defines the acceptability of Agency-wide spam protection tools as applied by the NASA Consolidated Email project manager.

3.15.2. Center Chief Information Security Officer (CISO)

CISO:

- Manages any Center-specific spam filtering measures used at their Center.

3.15.3. Information System Owner (ISO)

ISO:

- Implements spam protection for their site and/or system if it does not use the Agency enterprise-wide email service.
- Tailors spam controls for their system if it is an OT system.

3.16. Spam Protection | Central Management (SI-8(1))

3.16.1. NASA Consolidated Email Project Manager

NASA Consolidated Email Project Manager:

- Implements spam protections in the enterprise-wide email service using tools approved by the SAISO.

3.17. Spam Protection | Automatic Updates (SI-8(2))

3.17.1. NASA Consolidated Email Project Manager

NASA Consolidated Email Project Manager:

- Ensures that the enterprise-wide email service automatically updates its built-in spam protection mechanisms.

3.18. Information Input Validation (SI-10)

3.18.1. Information System Owner (ISO)

ISO:

- Ensures the execution of information system input validation testing, including:
  - Rules for validating syntax and semantics of information system input (e.g., character set, length, numerical range).
  - Prescreening inputs passed to interpreters to prevent content from being treated as system commands.

3.19. Error Handling (SI-11)

3.19.1. Information System Owner (ISO)

ISO:

- Ensures the identification of potential security-relevant information system error conditions.
- Ensures information systems generate error messages that provide information necessary for corrective action without revealing sensitive or potentially harmful information, including Personally Identifiable Information, account numbers, and passwords, that could be exploited by adversaries.
- Ensures error messages are only available to specifically authorized personnel.

3.20. Information Handling and Retention (SI-12)

3.20.1. Information System Owner (ISO) and Information System Security Officer (ISSO)

ISOs and ISSOs:

- Retains information for their systems in accordance with Agency information protection and records management policies.

APPENDIX A: ACRONYMS

ATO	Authorization to Operate
ASUS	Agency Security Update Service
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISO	[Center] Chief Information Security Officer
CSI	Cybersecurity Infrastructure
CSPD	Cyber Security and Privacy Division
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
HBK	Handbook
ICS	Industrial Control Systems
IDS	Intrusion Detection System
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
ITS	Information Technology Security
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OCIO	Office of the Chief Information Officer
OT	Operational Technology

RISCS	Risk Information Security Compliance System
SI	System Information and Integrity
SOC	Security Operations Center
SP	Special Publication
SSP	System Security Plan
US-CERT	United States Computer Emergency Readiness Team