



# IT Security Handbook

## System and Communications Protection

ITS-HBK-2810.18-01  
Effective Date: 20110506  
Expiration Date: 20130506  
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

ITS Handbook (ITS-HBK-2810.18-01)  
System and Communications Protection Handbook

Distribution:

NODIS

Approved

*Valarie Burks*

Valarie Burks  
Deputy Chief Information Officer for  
Information Technology Security

*May 6, 201*

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 Application Partitioning (SC-2).....	5
3 Security Function Isolation (SC-3).....	6
4 Information in Shared Resources (SC-4).....	6
5 Denial of Service Protection (SC-5).....	6
6 Boundary Protection (SC-7) .....	6
7 Transmission Integrity (SC-8).....	6
8 Transmission Confidentiality (SC-9).....	6
9 Network Disconnect (SC-10).....	7
10 Cryptographic Key Establishment and Management (SC-12).....	7
11 Use of Cryptography (SC-13).....	7
12 Public Access Protections (SC-14).....	7
13 Collaborative Computing Devices (SC-15) .....	7
14 Public Key Infrastructure Certificates (SC-17).....	7
15 Mobile Code (SC-18) .....	7
16 Voice over Internet Protocol (SC-19).....	8
17 Secure Name/Address Resolution Services (Authoritative Source) (SC-20).....	8
18 Secure Name/Address Resolution Services (Recursive or Caching Resolver) (SC-21) .....	8
19 Architecture and Provisioning for Name/Address Resolution Service (SC-22).....	8
20 Session Authenticity (SC-23).....	9
21 Fail in Known State (SC-24).....	9
22 Protection of Information at Rest (SC-28) .....	9
23 Information System Partitioning (SC-32).....	9
24 Organizationally Defined Values.....	10

## 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 System and Communications Protection (SC) 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 System and Communication control family relates to the protection of confidentiality, integrity, and availability of NASA information systems and NASA information as it flows between communications networks. The control family ensures the establishment of an effective physical and logical network security perimeter and provides guidance for best protecting information as it moves both within the security perimeter and as it moves to and from other networks outside the security perimeter such as the Internet.
- 1.7 **Applicable Documents**
- *NPD 2810.1, NASA Information Security Policy*
  - *NPR 1600.1, NASA Security Program Procedural Requirements*
  - *NPR 2810.1, Security of Information Technology*
  - *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
  - *OMB M-08-23, Securing the Federal Government's Domain Name System Infrastructure*
  - *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 800-21, Guideline for Implementing Cryptography in the Federal Government*
  - *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*
  - *NIST SP 800-58, Security Considerations for Voice over IP (VoIP) Systems*
  - *NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide*

## 2 Application Partitioning (SC-2)

- 2.1 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.

### 3 Security Function Isolation (SC-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 Information in Shared Resources (SC-4)

4.1 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.

### 5 Denial of Service Protection (SC-5)

#### 5.1 Roles and Responsibilities

5.1.1 *The ISO shall:*

5.1.1.1 Ensure the capability in information systems to limit the effects of denial of service attacks in a manner consistent with organizationally defined values.

### 6 Boundary Protection (SC-7)

#### 6.1 Roles and Responsibilities

6.1.1 *The ISO shall:*

6.1.1.1 Ensure managed interfaces for boundary protection of information systems are employed, monitored, audited and controlled at connection points to the Internet or other external networks and other key internal points using firewalls, routers, encrypted tunnels, or other security devices and/or processes.

6.1.1.2 Ensure information systems that are connected to external systems prevent public access into the NASA internal networks, except as appropriately mediated by managed interfaces employed by boundary protection devices.

6.1.1.3 Ensure the number of access points to NASA information systems is minimized to meet NASA mission requirements and to allow comprehensive monitoring of inbound and outbound communication and network traffic.

6.1.1.4 Ensure traffic flow policies are established and reviewed for each managed interface in a manner consistent with organizationally defined values.

6.1.1.5 Ensure the exceptions to the traffic flow policy are documented and reviewed in a manner consistent with organizationally defined values.

6.1.1.6 Ensure information systems prevent remote devices that have established a non-remote connection (e.g. VPN) with the system from communicating outside that path and with resources external to the network.

6.1.1.7 Ensure information systems prevent the unauthorized release of information outside the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

6.1.1.8 Ensure information systems route all internal traffic to the Internet through authenticated proxy servers within the managed interfaces of boundary protection devices in a manner consistent with organizationally defined values.

### 7 Transmission Integrity (SC-8)

7.1 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.

### 8 Transmission Confidentiality (SC-9)

8.1 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.

## 9 Network Disconnect (SC-10)

### 9.1 Roles and Responsibilities

#### 9.1.1 *The ISO shall:*

- 9.1.1.1 Ensure information systems automatically terminate connections in a manner consistent with organizationally defined values.
- 9.1.1.2 Ensure for remote sessions, information systems automatically terminate connections in a manner consistent with organizationally defined values.

## 10 Cryptographic Key Establishment and Management (SC-12)

### 10.1 Roles and Responsibilities

#### 10.1.1 *The ISO shall:*

- 10.1.1.1 Ensure COMSEC issuance and management controls are in accordance with the requirements in *NPR 1600.1*.
- 10.1.1.2 Ensure that, when required cryptography is employed for an information system, cryptographic key management is established.

## 11 Use of Cryptography (SC-13)

- 11.1 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.

## 12 Public Access Protections (SC-14)

- 12.1 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.

## 13 Collaborative Computing Devices (SC-15)

- 13.1 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.

## 14 Public Key Infrastructure Certificates (SC-17)

### 14.1 Roles and Responsibilities

#### 14.1.1 *The ISO shall:*

- 14.1.1.1 Ensure adherence to policy for the creation and issuance of federal credentials as defined by the Office of Protective Services (OPS).
- 14.1.1.2 Ensure that Public Key Infrastructure Certificates policies and requirements are followed for obtaining and using PKI certificates.
  - 14.1.1.2.1 NASA entered into an Agreement with the United States Treasury to have the United States Treasury as the Shared Service Provider for the operation of the NASA Certification Authority (CA), referred to as the NASA Operational Certification Authority (NOCA). Under this Agreement, NASA retains responsibility for the operation of the Registration Authorities (RAs).
  - 14.1.1.2.2 The NOCA is the collection of hardware and software and trusted roles used to issue certificates to Subscribers. The Federal PKI Common Policy governs the issuance and management of all NASA-issued PKI certificates. The NOCA may provide the following: certificate creation, certificate signing, certificate revocation, key management, and publication of certificate revocation lists (CRLs) and authority revocation lists (ARLs).
  - 14.1.1.2.3 The NASA PKI website, <http://pki.nasa.gov>, provides for new PKI requests, technical support, and other operational support information.

## 15 Mobile Code (SC-18)

### 15.1 Roles and Responsibilities

- 15.1.1 *The ISO shall:*
  - 15.1.1.1 Manage the use of mobile code technologies.
    - 15.1.1.1.1 The following mobile code and mobile code technologies are defined below as High Risk, Moderate Risk, and Low Risk:
      - a. High Risk: Mobile code technologies that exhibit functionality allowing unmediated access to host and remote system services and resources.
      - b. Medium Risk: Mobile code technologies that have functionality allowing mediated or controlled access to local system services and resources.
      - c. Low Risk: Mobile code technologies that have functionality with no capability for unmediated access to local system services and resources.
  - 15.1.1.2 Ensure usage restrictions and implementation guidelines for mobile code and mobile code technologies are limited to:
    - 15.1.1.2.1 Intranet Usage – Low, Medium, and High risk mobile code is permitted in controlled and trusted environments.
    - 15.1.1.2.2 Internet Server Usage – Externally facing web servers will be permitted to serve Low, Medium, and High risk mobile code due to the capabilities and functionality that mobile code technologies afford.
    - 15.1.1.2.3 Internet Client Usage – All High risk mobile code will be blocked or disabled (i.e. via web proxy with content filtering) for Internet browsing sessions.

## 16 Voice over Internet Protocol (SC-19)

### 16.1 Roles and Responsibilities

- 16.1.1 *The ISO shall:*
  - 16.1.1.1 Ensure Voice Over Internet Protocol (VoIP) is not used in NASA information systems unless:
    - 16.1.1.1.1 Fully documented in the SSP and approved by the AO;
    - 16.1.1.1.2 Approved by the contracting officer for the Agency telecommunication contracts; and
    - 16.1.1.1.3 It is not a violation of a NASA telecommunications contract.
  - 16.1.1.2 Ensure approved VoIP security and implementations are in accordance with NIST SP 800-58.

## 17 Secure Name/Address Resolution Services (Authoritative Source) (SC-20)

### 17.1 Roles and Responsibilities

- 17.1.1 *The ISO shall:*
  - 17.1.1.1 Ensure information systems use the NASA Domain Name System (DNS) infrastructure, through the NASA Integrated Services Network (NISN).

## 18 Secure Name/Address Resolution Services (Recursive or Caching Resolver) (SC-21)

### 18.1 Roles and Responsibilities

- 18.1.1 *The ISO shall:*
  - 18.1.1.1 Ensure the use of the NASA DNS infrastructure for all recursive name resolution, through NISN.

## 19 Architecture and Provisioning for Name/Address Resolution Service (SC-22)

### 19.1 Roles and Responsibilities

- 19.1.1 *The ISO shall:*
  - 19.1.1.1 Ensure DNS Servers providing name/address resolution service are fault tolerant and implement internal/external role separation.
  - 19.1.1.2 Ensure primary and secondary authoritative DNS servers are on separate subnets at separate locations.
  - 19.1.1.3 Ensure DNS servers with an internal role only process name/address resolution requests from internal clients.
  - 19.1.1.4 Ensure DNS servers with an external role only process name/address resolution requests from external clients.

19.1.1.5 Ensure the set of clients that can access the authoritative DNS servers are specified.

## **20 Session Authenticity (SC-23)**

20.1 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.

## **21 Fail in Known State (SC-24)**

### **21.1 Roles and Responsibilities**

21.1.1 The ISO shall:

21.1.1.1 Ensure information systems fail in a secure manner that preserves log data, last-user-logged-in data, connectivity information as well as ensuring the confidentiality, integrity, and availability of the resource in a manner consistent with organizationally defined values.

## **22 Protection of Information at Rest (SC-28)**

22.1 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.

## **23 Information System Partitioning (SC-32)**

23.1 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.

## 24 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
SC	01	System and Communications Protection Policy and Procedures	Main	[1]	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
SC	05	Denial of Service Protection	Main	[1]	Reference	List of attack types for which protection/mitigation is required.	Denial of Service (Note: As defined by <a href="https://www.us-cert.gov">https://www.us-cert.gov</a> )	Denial of Service (Note: As defined by <a href="https://www.us-cert.gov">https://www.us-cert.gov</a> )	Denial of Service (Note: As defined by <a href="https://www.us-cert.gov">https://www.us-cert.gov</a> )
SC	07	Boundary Protection	E 4	[1]	Frequency	Review of exceptions to traffic flow policies.		1/Year	1/Year
SC	07	Boundary Protection	E 8	[1]	Reference	List of internal traffic types for which proxy server routing is required.			All Internal Traffic
SC	07	Boundary Protection	E 8	[2]	Reference	List of external networks to which internal traffic must be routed through proxy servers.			Internet
SC	10	Network Disconnect	Main	[1]	Time Period	Inactive session termination.		At the end of a session; 30 Minutes of inactivity; 15 Minutes of inactivity for non-remote connections.	At the end of a session; 30 Minutes of inactivity; 15 Minutes of inactivity for non-remote connections.

ITS Handbook (ITS-HBK-2810.18-01)  
System and Communications Protection Handbook

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
SC	15	Collaborative Computing Devices	<i>Main</i>	[1]	Reference	List of exceptions to prohibiting remote activation of collaborative computing devices.	None	None	None
SC	24	Fail In Known State	<i>Main</i>	[1]	Reference	Known state.			Single-user; No network services available; Preservation of log data
SC	24	Fail In Known State	<i>Main</i>	[2]	Reference	List of types of failures.			a) "Flooding" and/or traffic overload of firewalls, networks or systems that cause it to fail (crash); b) Communication connectivity ; c) Hardware, e.g. server
SC	24	Fail In Known State	<i>Main</i>	[3]	Reference	List of information preserved following failure.			a) System logs; b) System backup data; c) System applications;