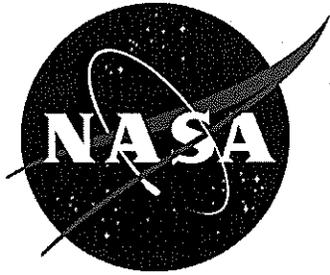


# **NASA Information Technology Requirement**



**NITR 2810-19**

Effective Date: November 12, 2008

Expiration Date: May 16, 2011

---

## **Audit and Accountability Policy and Procedures**

---

Responsible Office: Office of the Chief Information Officer

## Table of Contents

### Change History

### PREFACE

- P.1 PURPOSE
- P.2 APPLICABILITY
- P.3 AUTHORITY
- P.4 APPLICABLE DOCUMENTS
- P.5 MEASUREMENT AND VERIFICATION
- P.6 CANCELLATION

### 1.0 REQUIREMENT

- 1.1 Audit and Accountability Policy
- 1.2 Procedures

### APPENDIX A. Definitions

### APPENDIX B. Acronyms

### APPENDIX C. Organization Defined Values for the Audit and Accountability (AU) Security Controls

### Distribution

NODIS

## Change History

NITR-2810-19, Audit and Accountability Policy and Procedures

<b>Change Number</b>	<b>Date</b>	<b>Change Description</b>

## **PREFACE**

### **P.1 PURPOSE**

a. To provide the NASA information system audit and accountability policy and procedures to meet the current National Institute of Standards and Technology (NIST) requirements.

### **P.2 APPLICABILITY**

a. This NITR applies to unclassified information systems at NASA Headquarters and Centers, including Component Facilities and Technical and Service Support Centers. To the extent specified in their respective contracts or agreements, it applies to the NASA Jet Propulsion Laboratory, other contractors, grant recipients, or parties to agreements for information systems that they use or operate on behalf of the Agency or that support the operations and assets of the Agency.

### **P.3 AUTHORITY**

a. Reference Paragraph P.3, NPR 2810.1A.

### **P.4 APPLICABLE DOCUMENTS**

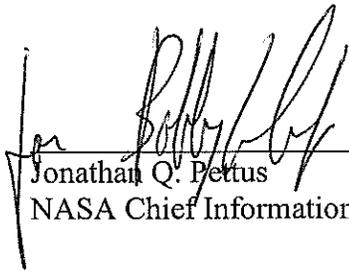
- a. NPR 2810.1, Security of Information Technology.
- b. NPR 1382.1, NASA Privacy Procedural Requirements.
- c. NPR 1600.1, NASA Security Program Procedural Requirements.
- d. NPD 2540.1, Personal Use of Government Equipment Including Information Technology (IT).
- e. Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.
- f. NIST SP 800-100, Information Security Handbook: A Guide to Managers.
- g. NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems.
- h. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.
- i. NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems.
- j. NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access.
- k. NIST SP 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.
- l. NIST SP 800-63, Electronic Authentication Guidelines.
- m. NIST SP 800-92, Guide to Security Log Management.

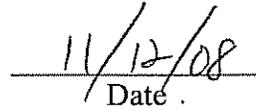
## P.5 MEASUREMENT AND VERIFICATION

- a. Annual certification of the Agency common security control AU-1, Audit and Accountability Policy and Procedures.
- b. Annual assessment of the Agency common security control AU-1 by the Information System Owner (ISO) as part of the system Continuous Monitoring requirements.

## P.6 CANCELLATION

- a. This NITR cancels and is a replacement for Chapter 21, *Audit Trail and Accountability*, of NPR 2810.1A, *Security of Information Technology*.
- b. The next version of NPR 2810.1 cancels this NITR.

  
Jonathan Q. Pettus  
NASA Chief Information Officer

  
Date .

## 1.0 REQUIREMENT

### 1.1 Audit and Accountability Policy

1.1.1 The NASA information and information system audit and accountability policy shall be consistent with applicable laws, Executive Orders, directives, regulations and guidance. The objective is to assure that there is information and information system audits to account for, respond to, and minimize the impact of incidents that can impact the information or information system.

1.1.2 Audit trails, used in conjunction with appropriate tools and procedures, shall be collected and utilized for individual accountability, reconstruction of events, intrusion detection, and problem identification. NIST SP 800-92 provides guidance on security log management.

1.1.3 All audit trail and accountability requirements identified in NIST 800-53, Revision 2 shall be implemented in all Agency information systems.

1.1.3.1 The amount of logging detail shall be commensurate with the information system security category.

1.1.4 The confidentiality of the log data and audit trail information shall be labeled and protected as Sensitive but Unclassified (SBU) in accordance NPR 1600.1, *NASA Security Program Procedural Requirements*.

1.1.5 Logs and other audit trails shall be reviewed periodically with the frequency of the reviews and retention schedule being consistent with the information system security category.

1.1.6 Access to audit logs shall be strictly controlled.

1.1.7 For Moderate and High security category information systems, there shall be a separation of duties between the security personnel who administer the access control and logging functions and those that administer the audit trail.

### 1.2 Procedures

1.2.1 The Information System Owner (ISO) shall:

a. Prepare system audit and accountability procedures implementing the above policy and requirements and document the procedures in the System Security Plan (SSP).

b. Assure the requirements of the NASA organizational defined values for the NIST 800-53, Revision 2 Audit and Accountability security controls are implemented and are included in the system audit and accountability procedures documentation. (Appendix C, *Organizational Defined Values for the Audit and Accountability (AU) Security Controls*.)

1.2.2 The Senior Agency Information Security Officer (SAISO) shall:

a. Annually review, and update as required, the Agency Audit and Accountability Control Policy and Procedures as part of the annual review of the AU-1 control as an Agency common control.

b. Annually certify the AU-1 Agency common control to assure it satisfies the purpose, scope, and compliance requirements for auditing and accountability.

1.2.3 The Security Operations Center (SOC) shall provide the Agency central incident reporting, analysis and management.

## APPENDIX A. Definitions

Term	Definition
Certification	A formal process for testing components or systems against a specified set of security requirements. Certification is normally performed by an independent reviewer, rather than one involved in building the system. Certification is more often cost-effective for complex or high-risk systems.
Common Control	A security control that is inherited by an information system
Continuous Monitoring	Refers to a phase of the Certification and Accreditation Process of Information Systems. It consists of three tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation. The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the authorizing official when changes occur that may impact on the security of the system. The activities in this phase are performed continuously throughout the life cycle of the information system.
Information System Owner	An agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. Responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the security requirements.
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operation, organizational assets, individuals, other organizations, and the Nation. [FIPS 199 as amended by NIST SP 800-53]
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544] Synonymous with Chief Information Security Officer (CISO)
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality,

<b>Term</b>	<b>Definition</b>
	integrity, and availability of the system and its information.
Site Control or Site Common Control	An inherited security control from a common site that usually applies to multiple information systems. Example is when more than one system is operating from a common data center (site) and information system owners are required to use that sites' security controls, e.g. site access control, site power, etc.

## **APPENDIX B. Acronyms**

ISO	Information System Owner
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NPR	NASA Procedural Requirements
SAISO	Senior Agency Information Security Officer
SBU	Sensitive But Unclassified
SOC	Security Operations Center
SSP	System Security Plan

**APPENDIX C. Organization Defined Values for the Audit and Accountability (AU)  
Security Controls**

Control	NIST 800-53 Security Control	Value for Low	Value for Moderate	Value for High
AU-2	The list of events that generate an audit record (AU-2)	Operating system settings from NIST: <a href="http://nvd.nist.gov/fdccc/index.cfm">http://nvd.nist.gov/fdccc/index.cfm</a>	Operating system settings from NIST: <a href="http://nvd.nist.gov/fdccc/index.cfm">http://nvd.nist.gov/fdccc/index.cfm</a>	Operating system settings from NIST: <a href="http://nvd.nist.gov/fdccc/index.cfm">http://nvd.nist.gov/fdccc/index.cfm</a>
AU-5	The actions to be taken in the event of an audit failure or audit storage capacity being reached [shutdown IS, overwrite oldest audit records, stop generating records]	Overwrite oldest audit records	Overwrite oldest audit records	Overwrite oldest audit records and, if capability exists, generate email notification
AU-5(1)	The percentage of storage capacity that causes the audit system to automatically generate a warning [i.e., warning generated when this percentage is reached]	N/A	N/A	80%
AU-5(2)	Audit failure events that cause the audit system to automatically generate a real-time alert [i.e., real time alert generated when this audit failure event occurs]	N/A	N/A	1. Hardware failures and/or errors 2. Software failures and/or errors 3. Audit storage capacity exceeded 4. System backup storage capacity exceeded
AU-6(2)	Inappropriate or unusual activities with security implications that cause automatic alert of security personnel	N/A	1. Blacklist Hit 2. Privilege Escalation	1. Blacklist Hit 2. Privilege Escalation 3. Security policy change
AU-8(1)	Frequency internal information system clocks are synchronized		Daily	Daily
AU-11	The time period that audit logs are retained	1 year then: Delete/destroy when not longer needed for administrative, legal, audit or other operational purposes (NPR 1441.1)	1 year then: Delete/destroy when not longer needed for administrative, legal, audit or other operational purposes (NPR 1441.1)	1 year then: Delete/destroy when not longer needed for administrative, legal, audit or other operational purposes (NPR 1441.1)