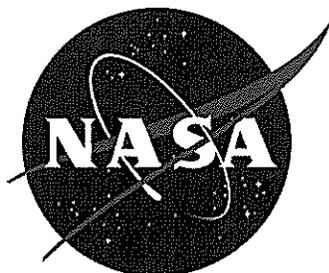


# NASA Information Technology Requirement



**NITR 2810-12**

Effective Date: May 18, 2008

Expiration Date: May 18, 2011

---

## **Continuous Monitoring**

---

Responsible Office: Office of the Chief Information Officer

## **Table of Contents**

### **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 General
- 1.2 Configuration Management and Control
- 1.3 Security Control Monitoring
- 1.4 Status Reporting and Documentation

### **2.0 RESPONSIBILITIES**

- 2.1 Senior Agency Information Security Official (SAISO)
- 2.2 Center Chief Information Officer (CIO)
- 2.3 Center Information Technology Security Manager (ITSM)
- 2.4 Information System Owner (ISO)
- 2.5 Authorizing Official (AO)
- 2.6 Authorizing Official Designated Representative (AODR)

### **APPENDIX A. Definitions**

### **APPENDIX B. Acronyms**

### **Distribution:**

### **NODIS**

## Change History

Change Number	Date	Change Description

## **PREFACE**

### **P.1 PURPOSE**

- a. This NASA Information Technology Requirement (NITR) describes the Agency procedural requirements and responsibilities for implementation of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 2, CA-7 Continuous Monitoring security control for NASA information systems.
- b. This NITR provides Agency continuous monitoring security assessment implementation and reporting instructions to satisfy NASA policy directives, Office of Management and Budget (OMB) directives, and NIST standards/requirements. It applies to all Federal Information Processing Standards (FIPS) Publication 199, security categories.
- c. This NITR is an addendum to NASA Procedural Requirements (NPR) 2810.1A, Security of Information Technology.

### **P.2 APPLICABILITY**

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**

Reference Paragraph P.3, NPR 2810.1A

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

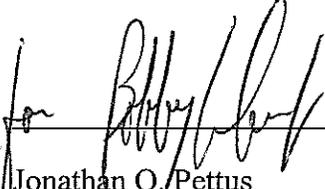
- a. NPR 2810.1A, Security of Information Technology
- b. Federal Information Processing (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems
- c. NIST SP 800-100, Information Security Handbook: A Guide to Managers
- d. NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems
- e. NIST SP 800-53A, DRAFT Guide for Assessing the Security Controls in Federal Information Systems
- f. NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems

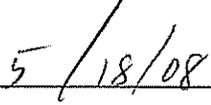
**P.5 MEASUREMENT AND VERIFICATION**

- a. The Agency-level measurement is the percentage of Agency systems, either NASA-owned or contractor-owned processing NASA data, that have had an annual security control assessment conducted as required for the annual Federal Information Security Management Act (FISMA) report.
- b. The Center-level measurement is the percentage of Center systems, either NASA-owned or contractor-owned processing NASA data, that have had an annual security control assessment conducted as required for the annual FISMA report.
- c. The Information System Owner (ISO) measurement is the number of security controls that were assessed during that fiscal year against the number of security controls that were required to be assessed for the annual assessment for that information system.

**P.6 CANCELLATION**

The next version of NPR 2810.1 cancels this NITR.

  
Jonathan Q. Pettus  
NASA Chief Information Officer

  
Date

## **1.0 REQUIREMENT**

### **1.1 General**

NASA Centers and Information System Owners (ISO) shall meet the continuous monitoring requirements of NIST 800-37 and NIST 800-53 Revision 2 CA-7 Continuous Monitoring security control assessments for all information systems.

1.1.1 The current fiscal year's assessment results obtained during continuous monitoring may be used to meet the annual FISMA requirement of the CA-2 Security Assessments security control.

1.1.2 For FIPS 199 Moderate and High systems, unless conducted by an independent Certification Agent (CA), the continuous monitoring assessment results shall not be used for the CA-4 Security Certification security control assessments.

1.1.3 The information system annual security control assessment shall be based on the fiscal year and will be completed not later than July 31<sup>st</sup>.

1.1.4 The RMS C&A Documentation Repository and POA&M Management System, referred to as RMS, shall be used to document information system continuous monitoring security control assessments.

1.1.5 According to NIST SP 800-37, continuous monitoring applies to information systems and consists of three tasks:

- a. Configuration management and control
- b. Security control monitoring
- c. Status reporting and documentation

### **1.2 Configuration Management and Control**

The ISO shall:

- a. Document proposed or actual changes to the system including hardware, software, firmware, and surrounding environment.
- b. Analyze the proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment) to determine the security impact of such changes.
- c. If the analysis determines that there is a significant change requiring reaccreditation of the information system, report the system security status to the Center Information Technology Security Manager (ITSM) and the Authorizing Official (AO).

### 1.3 Security Control Monitoring

1.3.1 A schedule shall be established by the ISO for continuous monitoring security control assessment to ensure that all controls requiring annual assessment are covered and that all controls are assessed at least once during the three-year accreditation cycle:

- a. Year 1 – Full accreditation, all security controls assessed.
- b. Year 2 – All security controls required to be assessed annually (see Table 1 below), plus a subset of the remainder of security controls must be assessed.
- c. Year 3 – All security controls required to be assessed annually (see Table 1 below), plus a subset of security controls that were not assessed during Year 2 must be assessed.

1.3.1.1 When a system is Certified and Accredited, it is considered to have met the annual continuous monitoring security control assessment requirement for that fiscal year.

1.3.2 As it is not feasible or cost-effective to monitor all of the security controls in an information system on a continuous basis, an appropriate subset of those controls for the annual assessment shall be selected.

1.3.2.1 The selection of a subset of security controls by the SAISO, Center CIO, and ISO for continuous monitoring assessment includes the following considerations:

- a. Annual Security Control Requirements – Those security controls that require annual assessment as identified by NIST SP 800-53.
- b. Significant changes to an information system – A significant change to an information system, or its operating environment, may introduce new security vulnerabilities and may require a more frequent assessment of select security controls.
- c. External influences – Activities outside the direct control of the information system which may impact security posture. Examples may include, but are not limited to, organizational changes, new or modified policies, and newly identified threats or vulnerabilities.
- d. Agency requirements – Those security controls that the Agency deems essential to protecting the information system may require increased attention, and more frequent assessment.
- e. Plan of Action and Milestone (POA&M) items – New or modified security controls, implemented to remediate identified weaknesses, should be assessed for effectiveness.

1.3.3 The security controls listed in Table 1 below shall be assessed at least annually:

Information System Security Controls Requiring Annual Assessment	Responsible for Assessment	An individual FISMA Reportable Action Item
--	----------------------------	--

Agency Common Controls (AC-1, AT-1, AT-4, AU-1, CA-1, CM-1, CP-1, CP-8, IA-1, IR-1, IR-5, IR-7, MA-1, MP-1, PE-1, PL-1, PL-4, PS-1, SC-1, RA-1, SA-1, SA-4, SI-1, SC-17)	Agency	No
Agency Hybrid Controls [Part of Agency Common Controls] (AC-18, AC-19, AC-20, CM-6, IR-2, IR-3, SC-12, SC-18, SC-19, SI-4, SI-5)	Agency and Center	No
Contingency Planning (CP) security controls (CP-2; CP-3; CP-4; CP-5; CP-6; CP-7; CP-9; CP-10)	Center	CP-4 (Test/Exercise of Contingency Plan)
Security Awareness Training (AT) security controls (AT-2)	Center	Yes
Configuration Management (CM) security controls (CM-2; CM-3; CM-4; CM-5; CM-7; CM-8)	Center	No
Plan of Action and Milestone (POA&M) Security Control (CA-5)	Center	Yes
Critical or volatile security controls, as determined by the ISO	Center	No
For a Center's information systems, the Center CIO may identify Center or Site Common Controls and/or designate additional security controls for annual assessment	Center	No

Table 1. Security Controls Requiring Annual Assessment

1.3.4 The selected subset of security controls shall be assessed by the ISO to determine the extent to which the controls are implemented correctly, operating as intended, and producing the

desired outcome with respect to meeting the security requirements for the information system in accordance with NIST SP 800-37, paragraph 3.4, subtask 9.2.

#### **1.4 Status Reporting and Documentation**

1.4.1 The ISO shall:

- a. Document the results of the continuous monitoring security control assessments in RMS.
- b. Document deficiencies or weaknesses identified during the continuous monitoring security control assessment process in RMS.
- c. Update the system security plan to reflect the proposed or actual changes to the information system.
- d. If a determination is made that reaccreditation is required (i.e., a significant change), document in RMS as a failure of the CA-6, Security Accreditation, security control.

### **2.0 RESPONSIBILITIES**

#### **2.1 Senior Agency Information Security Official (SAISO)**

2.1.1 The SAISO shall:

- a. Provide oversight to the Center Information Technology Security Managers (ITSM) on continuous monitoring security control assessment procedures.
- b. Ensure Agency common security controls (as designated by the SAISO) are certified annually.
- c. Prepare and submit Agency metrics on continuous monitoring security control assessments as required for the annual Federal Information Security Management Act (FISMA) report.

#### **2.2 Center Chief Information Officer (CIO)**

2.2.1 The Center CIO shall:

- a. Ensure completion of continuous monitoring security control assessments on all Center information systems.
- b. Ensure Center CIO designated site and/or common security controls are certified annually.

#### **2.3 Center Information Technology Security Manager (ITSM)**

2.3.1 The Center ITSM shall:

- a. Provide oversight to continuous monitoring security control assessment activities for Center information systems, ensuring completion and reporting no later than July 31<sup>st</sup> of each fiscal year.

- b. Provide an assessment and recommendation to the ISO and the Authorizing Official (AO) as to the need for reaccreditation as a result of a reported or identified significant change to a Center information system.
- c. Prepare and submit Center metrics on continuous monitoring security control assessments as required for the annual FISMA report to the SAISO.

## **2.4 Information System Owner (ISO)**

2.4.1 The ISO may designate a representative to perform continuous monitoring security control assessment activities, but retains the responsibility for completion, quality, and reporting.

2.4.2 The ISO shall:

- a. Be Responsible for continuous monitoring security control assessment activities described in section 1.0.
- b. Ensure resources are provided for the continuous monitoring security control assessment activities for all information systems which they are responsible.
- c. Report to the Center ITSM and AO, any significant changes made to an information system for which they are responsible that may cause an impact to the security status and require a reaccreditation of the system.

## **2.5 Authorizing Official (AO)**

2.5.1 The AO may designate an Authorizing Official Designated Representative (AODR) to support the AO in continuous monitoring security control assessment activities and responsibilities in accordance with NIST SP 800-37, paragraph 2.2.

2.5.1.1 The AODR designation shall be in writing, identify the empowerment granted by the AO, and signed by the AO. The only activity that cannot be delegated by the AO is the security accreditation decision and the signing of the associated accreditation decision letter.

2.5.2 May designate an individual other than the ISO to perform the continuous monitoring security control assessments and implement the actions required in section 1.0.

2.5.3 The AO shall:

- a. Determine whether a significant change to an information system requires reaccreditation and advise the ISO of such a decision.
- b. Review information system security weaknesses reported in the RMS tool that was identified during the continuous monitoring security control assessment activities.

## **2.6 Authorizing Official Designated Representative (AODR)**

2.6.1 The AODR shall be responsible for all continuous monitoring security control assessment activities as designated in writing by the AO.

## Appendix A. Definitions

Term	Definition
Authorizing Official	A NASA official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals.
Authorizing Official Designated Representative	Individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.
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.
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.
Plan of Action and Milestones	The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. POA&Ms are used to close security performance gaps, assist the Inspector General (IG) in their evaluation work of agency security performance, and assist OMB with oversight responsibilities.

Term	Definition
RMS C&A Documentation Repository and POA&M Management System	A SecureInfo Corporation application used as the Agency's enterprise tool to document and track all Agency information system certification and accreditation, security control assessments and both system and programmatic vulnerabilities and weaknesses.
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, integrity, and availability of the system and its information.
Significant Change	Examples of significant changes to an information system that should be reviewed for possible reaccreditation include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform or firmware component; or (iv) modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reaccreditation action.
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.
Volatile or critical Security Controls	Those security controls that may be considered more critical than other controls because of the potential impact on the information system if these controls were subverted or found to be ineffective.

## **Appendix B. Acronyms**

AO	Authorizing Official
AODR	Authorizing Official Designated Representative
AT	Awareness and Training
C&A	Certification and Accreditation
CIO	Chief Information Officer
CM	Configuration Management
CP	Contingency Planning
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
ISO	Information System Owner
IT	Information Technology
ITSM	Information Technology Security Manager
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
RMS	Risk Management System C&A documentation Repository and POA&M Tracking System
SAISO	Senior Agency Information Security Official
SOP	Standard Operating Procedure
SP	Special Publication