

National Aeronautics and
Space Administration
Headquarters
Washington, DC 20546-0001



JAN 31 2006

Reply to Attn of: **Office of the Chief Information Officer**

TO: Distribution

FROM: NASA Chief Information Officer

SUBJECT: Review and Approval of Changes to Information Technology Baseline

Effective immediately, I have established a requirement for review and approval of changes to NASA's information technology (IT) and systems baseline. A copy of that memorandum is enclosed. I am delegating to each Center Chief Information Officer (CIO) the responsibility, authority, and accountability to review and approve all changes to all IT systems (program unique, multi-program and general purpose) residing at their Center, based on the list of systems in their Center's ITS Registry of systems used to provide status information in the Center's Federal Information Security Management Act (FISMA) reports.

Examples of significant changes to an information system 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. Areas of particular concern are new or modified network connections or trust relationships of the Center's or Program Active Directory infrastructure and local area network and wide area network (WAN) and external connections.

All modifications to a NASA IT system that significantly changes the system are required to be reviewed by the Center CIO to determine the appropriateness of the action based on the nature of the change. Types of changes that are allowed: response to a known IT security incident; keeping existing systems operating in accordance with existing configuration control processes. For IT systems which impact more than one Center, the cognizant Center CIO's are responsible and accountable for coordinating their mutual review and approval. Each Center CIO is expected to use their best judgment in authorizing any changes, and to report to Mr. Michael Castagna of the Office of the CIO all changes they have approved. The Center CIO's will follow the Standard Operating Procedure (SOP) enclosed.

The requirement to track and document significant changes to a system is not new and is part of the existing process for managing all Agency systems as per NPR 2810. The review, approval and reporting process will continue until otherwise notified.

Signature on File
Patricia L. Dunnington

Enclosure

DISTRIBUTION:

Center Chief Information Officers:

ARC/S. Longchamps (Acting)

DFRC/R. Binkley

GRC/S. Pillay

GSFC/P. Hunter (Acting)

Headquarters/S. Daniels-Gibson

JPL/J. Rinaldi

JSC/J. Carter

KSC/B. Hevey

LaRC/C. Mangum

MSFC/J. Pettus (Acting)

SSC/G. Irby (Acting)

cc:

Mission Directorate Chief Information Officers:

Space Operations/C. Pino

Aeronautics Research/G. Cox (Acting)

Science/J. Bredekamp

Exploration Systems/C. McCaslin

National Aeronautics and
Space Administration

Headquarters

Washington, DC 20546-0001



JAN 31 2006

Reply to Attn of:

Office of the Chief Information Officer

TO: Officials-in-Charge of Headquarters Offices

FROM: NASA Chief Information Officer

SUBJECT: Review and Approval of Changes to Information Technology Baseline

There are several initiatives currently underway at NASA to improve the interoperability, reliability, security, and management of information technology (IT) and systems across the Agency, such as the Wide Area Network Replacement (WAN-R) project, NASA Integrated Security Environment (NISE) project, and the NASA Portal project. As well, there are several directives on the horizon that will significantly affect NASA's IT and systems environment, such as Homeland Security Presidential Directive -12 and the transition to Internet Protocol version 6 (IPv6). These initiatives and directives, while challenging to implement, provide NASA the opportunity to improve the management and security of IT and systems across the Agency. The successful integration of these important initiatives is reliant on effective configuration control and prioritization of investments at the Agency level to minimize duplication and maximize effectiveness of Agency-wide efforts.

Therefore, effective immediately, no significant changes to any of NASA's existing IT and systems, including applications, networks and infrastructure, in all three portfolios (program unique, multi-program and core/general purpose) shall be undertaken without review and approval by the NASA Chief Information Officer (CIO) or the cognizant Center CIO. Approval is required for any and all significant modifications, acquisitions, upgrades, or other changes, to information systems within, or interconnected to, the NASA environment, whether by the government or contractors.

I have delegated to each Center's CIO, the responsibility, authority, and accountability to review and approve change requests for all IT and systems that reside at their respective Center, component facilities, or that are connected to a network at their Center. Where the Center CIO is unable to ascertain the appropriateness of a change, the change request will be forwarded to the NASA CIO for review and approval. The Center CIO's have been provided additional guidance regarding what constitutes a significant change and information that is required to request a change approval. The requirement to track and document significant changes to a system is not new and is part of the existing process for managing all Agency systems as per NPR 2810. This change review process will remain in effect until withdrawn in writing.

I appreciate your assistance in supporting this change review process and in communicating these requirements to those who report to you. By working together, we can improve the confidentiality, availability, and integrity of our information technology and systems.

Thank you for your support.

Patricia L. Dunnington



NASA Standard Operating Procedure

Procedures for Approving Changes to NASA's Information Technology Baseline

ITS-SOP-tbd

Effective Date: tbd

Expiration Date: tbd

Responsible Office: AO / Chief Information Officer

Procedures for Approving Changes to NASA's Information Technology Baseline

Objective:

With the ever increasing challenges posed by today's cyber threats, the Agency must maintain a solid understanding of the configuration of NASA's information technology and systems. Many seemingly insignificant changes at various Centers, in aggregate can lead to major vulnerabilities that expose NASA's information and systems to unacceptable risks. A consistent and repeatable processes for review, approval and reporting is required to demonstrate that the appropriate due diligence is performed. Center CIOs have been delegated the responsibility, authority and accountability for review and approval of all changes to all IT systems (program unique, multi-program and general purpose) at their Centers. This Standard Operating Procedure (SOP) is to ensure that NASA has consistent and repeatable processes for review, waiver, approval, and reporting of changes to all NASA IT and systems. This SOP provides maximum flexibility at the Center level, while assuring effective oversight by the NASA CIO.

This review, approval and reporting mechanism makes use of existing certification and accreditation (C&A) processes. The requirement to track and document significant changes to a system is part of the existing continuous monitoring process for managing all Agency systems per NPR 2810.1.

References:

1. Security of Information Technology (NASA Procedures and Requirements (NPR) 2810.1)
2. Guide for the Security Certification and Accreditation of Federal Information Systems (NIST SP 800-37)
3. Risk Management Guide for Information Technology Systems (NIST SP 800-30)
4. Standards for Security Categorization of Federal Information and Information Systems (FIPS 199)

Definitions:

Authorization Official: 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. See NPR 2810.1, Chapter 14, for the assignment of Authorizing Officials within NASA.

Plans of Action and Milestones (POA&M): A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Significant Change: Significant changes to an information system 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

Implementation:

1. Each Center CIO is responsible and accountable to:
 - 1.1. Develop and maintain a list of changes that the Center CIO does not judge to be significant changes and, therefore, intends to waive from the review process. The Center CIO shall submit that list, and subsequent changes to that list, to Mr. Michael Castagna, Office of the NASA CIO, for approval.
 - 1.2. Review and approve all significant changes to all systems residing at their Center, based on the list of systems in their Center's IT Security Registry. Center CIOs must work with Authorizing Officials in the review and approval of requests for all significant changes. Reporting requirements are specified below.
2. Change requests shall document proposed changes to the information system by using established Center configuration management and control procedures. See reporting section below for format and content.
3. Change requests shall include a security impact analysis that shows how security will be affected by the requested change. This analysis is essential since changes can introduce new vulnerabilities or affect required security controls. If the security impact analysis reveals that the changes will impact security, the system's Plans of Actions and Milestones (POA&M) should be updated with corrective actions and the Authorizing Official must decide if a recertification is warranted. A security impact assessment must be performed so that the level of effort is commensurate with the information system's FIPS 199 data categorization. The development of a security impact analysis is a derivative of the preparation and update of a risk assessment. The security impact analysis should be based on NIST 800-30, Risk Management Guide for Information Technology Systems, and should be structured in the following manner: (Further detail can be obtained in Chapters three and four of NIST 800-30)
 - a. Executive Summary (highlighting the residual risk that exists after appropriate security controls are applied)
 - b. Likelihood Determination (section 3.5)
 - c. Impact Analysis (section 3.6)
 - d. Risk Determination (section 3.7)
 - e. Control Recommendations (section 3.8)
 - f. Risk Mitigation Strategy (section 4.2)
3. Authorizing Officials that have systems that span multiple Centers are required to submit a request to the CIO at each Center that needs to undergo the significant change.

4. All modifications to a NASA IT system that significantly changes the system are required to be reviewed by the Center CIO to determine the appropriateness of the action based on the nature of the change. Particular areas of concern are new or modified network connections or trust relationships of the Center's or Program Active Directory infrastructure and local area network and wide area network (WAN) and external connections.

5. The types of changes that are allowed stem from known IT security vulnerabilities or incidents and maintaining existing systems in operation in accordance with existing configuration control processes. Each CIO is expected to review each request and associated security impact analysis and appropriately coordinate with Center security configuration control boards.

Reporting:

Reporting is required and should be sent to the Mr. Michael Castagna, NASA IT Security Officer on the second and fourth Tuesday of each month. The reporting shall include the following:

1.0 General Information

1.1 Center Name:

1.2 Date:

1.3 CIO Name:

2.0 Change Request Information

2.1 Center Change request number

2.2 System name and ITS number from the ITS Registry

2.3 Clear and brief description of the mission requirement that necessitates the change.

2.4 Clear and brief description of the change being requested.

2.5 Clear and brief description of the security impact

2.6 Recertification decision

2.7 Technical point of contact for the system

3.0 Decision:

3.1 Decision comments/rationale: (Approved/Disapproved)

3.2 Center CIO Signature:

3.3 Date :

Escalation:

The NASA CIO shall have final authority for escalation of change requests, decisions or reversal of change decisions.