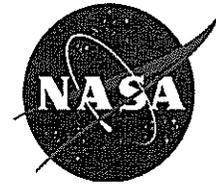


National Aeronautics and
Space Administration
Headquarters
Washington, DC 20546



OCT 30 2009

Office of the Chief Information Officer

TO: Distribution

FROM: Deputy CIO for Information Technology Security

SUBJECT: Implementation Plan for NIST SP 800-53, Revision 3 Security Controls

With the publication of NIST 800-53, Revision 3 in August 2009, supporting guidance concerning the Agency's implementation of the changes in Revision 3 is needed. Agencies are expected to be in compliance with NIST standards and guidelines within one year of the publication date, unless otherwise directed by the Office of Management and Budget (OMB). The one year compliance date for revisions to NIST publications applies only to the new and/or updated material in the publications. For information systems under development or for legacy systems undergoing significant changes, agencies are expected to be in compliance with the NIST publications immediately upon deployment of the information system.

The most recent revision to NIST SP 800-53 is significant both in breadth and depth. The increased number in baseline security controls derives from expanded and more detailed coverage of information technology to include security controls that address security programs as well as information systems. The depth in which a security control impacts an information system has also expanded and is most apparent through the increase of "supplemental guidance" and "control enhancements." All NASA personnel involved with assuring the security of information systems need to review and comply with NIST SP 800-53, Revision 3.

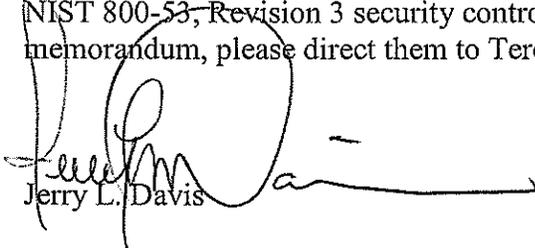
In accordance with NIST and OMB requirements, all NASA systems, internal and external, must be in compliance with NIST 800-53, Revision 3 by July 31, 2010. While agencies are required to follow NIST standards and guidelines, there is flexibility in how agencies apply the guidance. The following supporting guidance is provided in complying with the applicable provisions of NIST SP 800-53, Revision 3:

1. For legacy systems under an existing authorization to operate (ATO), compliance with new/updated material is required within one year of the NIST 800-53 publication date. However, the Agency is taking a phased approach to assessing Revision 3 security controls until the system is due for its 3-year authorization cycle or if a significant change has taken place. Independent certification of changed or new Revision 3 controls is not required. Self-assessment and risk acceptance is allowed until the next re-authorization milestone. Information System owners (ISOs) will document annual compliance requirements in RMS by running a NASA C&A Questionnaire-Oct 2009, and recording implementation details for required and selected Revision 3 security controls. ISOs will

need to look at all the revision 3 changes in order to assess the impact to their information systems and select those most critical for testing. If applicable a new Plan of Action and Milestone (POA&M) and Acceptance of Risk should be presented to the Authorizing Official (AO) for approval.

- a. For information systems due for re-authorization through February 2010, they may still conduct security controls testing using Revision 2 security controls. Self assessment of Revision 3 security controls will be based on required and ISO selected security controls.
 - b. For those due March 2010 and after, they shall conduct security controls testing using Revision 3 security controls.
 - c. Please see FAQ sheet number 14 for additional information.
2. For new systems, compliance with Revision 3 security controls is required immediately upon deployment of the system. However, for those systems that have been in development for awhile and have been implementing Revision 2 controls throughout the various life cycle development phases, costs to implement Revision 3 must be taken into consideration and if applicable, risk acceptance of not implementing Revision 3 controls must be approved by the AO.
 3. RMS, the official NASA Security Assessment and Authorization Repository (NSAAR) tool, will be populated with NIST SP 800-53, Revision 3 security controls by November 2, 2009.
 4. No additional Agency common controls from Revision 3 will be designated at this time. Review and selection of all Agency common controls will occur in June 2010. Please check with your Center ITSM as to when the Center site common controls will be updated to Revision 3.

Frequently Asked Questions (FAQs) to clarify this guidance regarding the implementation of NIST 800-53, Revision 3 security controls are attached. For questions regarding this memorandum, please direct them to Teresa Fryer at 202-358-2177 or teresa.fryer-1@nasa.gov.



Jerry L. Davis

Enclosure

DISTRIBUTION:

Center CIOs:

ARC/Chris Kemp
DFRC/Robert Binkley
GRC/Dr. Sasi Pillay
GSFC/Linda Cureton
HQ/Les Newell
JPL/Jim Rinaldi
JSC/Larry Sweet
KSC/Mike Bolger
LaRC/Cathy Mangum
MSFC/John McDougle (Acting)
SSC/Gay Irby
NSSC/Terry Jackson

Mission Directorate CIOs:

Aeronautics/Phil Milstead (Acting)
Exploration/ Beverly Hamilton
Science/Joe Bredekamp
Space Operations/Dan Hedin (Acting)

Center ITSMs

ARC/Ernest Lopez
DFRC/Larry Johnson
GRC/Don Cannatti
GSFC/Joshua Krage
HQ/Greg Kerr
JPL/Jay Brar
JSC/Ted Dyson
KSC/Henry Yu
LaRC/Kendall Freeman
MSFC/Walter Franklin
SSC/Christine Reynolds
NSSC/James Cluff

Enclosure: Frequently Asked Questions (FAQs) regarding NIST SP 800-53, Revision 3 Security Control Implementation

1. How do I know which security controls are changed by NIST SP 800-53, Revision 3?

An annotated NIST SP 800-53 is available on the NIST Special Publications library at [800-53-rev3-final_markup-rev2-to-rev3.pdf](#). The baseline of security controls has been extended from 154 required controls (plus 59 enhancements) for a Moderate-level system to 161 required controls (with 94 enhancements) for a High-level system under revision 3.

2. How do I select, assess, and certify Revision 3 controls into my information system which is already accredited using Revision 2 security controls? What are the RMS procedures to document this process?

The procedure includes running a NASA C&A Questionnaire-Oct 2009 questionnaire which automatically selects the baseline set of security controls based on your FIPS-199 system's impact level. When running the NASA C&A Questionnaire-Oct 2009 when you get to question 900 select Option 2 and then select Yes to question 905 "Do you want to generate a "System Security Plan" template. All other questions will be no. This will then generate a new System Security Plan (SSP) Revision 3. The ISO will review the Revision 3 security controls, document and implement the controls at a level of assurance commensurate with the current risk. The security control implementation would be self-assessed with review and authorization decision made by the system's Authorizing Official (AO). The self assessment will suffice until full certification at next authorization milestone. Assessment results would be reported in a Security Assessment Report (SAR) with security control test and test results posted to RMS using the Requirement Traceability Matrix (RTM).

3. Does RMS support both NIST SP 800-53, Revision 2 and Revision 3 security controls?

The RMS questionnaire used to create a SSP and other Assessment and Authorization (formerly known as C&A) supporting documents will only support one NIST SP 800-53 revision of security controls. Currently Revision 2 is supported. After November 2, 2009, only Revision 3 security controls will be available when generating a new package. Existing SSPs that were created using Revision 2 security controls will continue to be available in RMS after November 2, 2009 and will still be the official Authorization package until the next reauthorization milestone.

4. What if I have implementation detail in Revision 2 and it is still accurate for Revision 3?

In RMS, copy and paste the information from the Revision 2 SSP into Revision 3 SSP.

5. For External (contractor) information systems, when does that system have to comply with NIST SP 800-53, Revision 3 and how is the authorization documented?

ITS-SOP-0033 is being revised to document procedures that support NIST SP 800-53, Revision 3. As with NASA internal systems, NASA contractor information systems that provide external services must comply with FISMA. Supporting documentation must be made available by the contractor, reviewed and assessed by a responsible NASA

representative and approved by a NASA AO. The contractor system details and authorization activities will be recorded in RMS.

6. **Will the new Program Management (PM) category of security controls need to be incorporated into each system's SSP?**

No, these program level controls will be addressed at the Agency level with support from applicable Centers. They do not need to be incorporated into individual system SSPs. They are not considered Agency common controls.

7. **Will there be new designated Agency or Center common controls based on the Revision 3 updates? Will they be assessed, certified and available in RMS?**

No additional Agency common controls from Revision 3 will be designated at this time. Review and selection of all Agency common controls will occur in June 2010. Please check with your Center ITSM as to when your Center site controls will be updated to Revision 3. Note: Ames Center site controls have not been updated.

8. **When will the new guidance on agency defined values be issued, and will it afford any degree of system-specific refinements?**

Selected organizational defined values will be published November 2009. As described in NIST SP 800-53, tailoring of baseline security controls does provide for system-specific refinements. "After selecting the initial set of baseline security controls ..., the organization initiates the tailoring process to appropriately modify and more closely align the controls with the specific conditions within the organization (i.e., conditions specific to the information system or its environment of operation). The tailoring process includes ...Specifying *organization-defined parameters* in the security controls via explicit assignment and selection statements". Reference NIST SP 800-53, Revision 3, p 19.

9. **For the required information system security control assessments, who can approve, and what are the requirements, for the security control assessor (SCA) (formally certification agent)?**

a. For Low-impact security category information systems that are being assessed to obtain an Authorization to Operate (ATO) decision, the Authorization Official (AO) determines the degree of independence required and approves the SCA.

b. For low-impact security category information systems that are being assessed to meet the requirement for annual security control assessment, the AO does not need to approve the SCA as long as they are not considered part of the 3 year reauthorization assessment.

c. For Moderate- and High-impact security category information systems being assessed to obtain an ATO decision, the assessor must be a SAISO approved, independent SCA.

d. For Moderate- and High-impact security category information systems being assessed, to meet the requirement for annual security control assessment, the AO does not

need to approve the SCA as long as they are not considered part of the 3 year reauthorization assessment.

10. Can the annual security control assessments be used for/as the assessment for the ATO decision?

a. For Moderate- and High-impact security category information systems, unless the annual security control assessments were performed by a SAISO approved independent SCA, the annual security control assessments shall not be used for the reauthorization.

b. For Low-impact security category information systems, unless the AO makes a determination as to the level of independence of the SCA and approves the SCA, the annual security control assessments shall not be used for reauthorization.

11. Can the Information System Security Official (ISSO) be designated as the SCA?

For a Low-impact security category information system, the ISSO may be designated by the AO as the SCA for the information system assessment.

12. For an information system that needs to be re-authorized before the Revision 3 security controls are available in RMS, am I required to meet the NIST SP 800-53 Revision 3 security control requirements?

The 800-53, Revision 3 requirements do not go into effect until the template is available in RMS. Revision 2 security controls may still be used for information systems due to be reauthorized before March 1, 2010. Self assessment of Revision 3 security controls will be based on required and information system owner selected security controls. However, security control assessments conducted after that date shall be done using Revision 3 security controls.

13. If an information system is authorized to operate based on NIST 800-53, Revision 2 and won't need reauthorization until FY11 (or FY12), can I use the Revision 2 security controls for the required FY10 annual security control assessments?

No, the required and selected annual security controls assessments must be conducted using Revision 3 security controls for FY10 and after. However, full independent assessment of Revision 3 security controls does not occur until the system's 3 year Authorization milestone or a significant system change occurs that requires reauthorization.

14. How will running a second questionnaire impact the RTM in RMS?

a. Is any data lost?

No, data is not lost. When a NASA C&A Questionnaire-Oct 2009 questionnaire is run to create another SSP template, the existing SSP is not affected. In the "Documents" folder both SSP will be available for use.

b. Is a second RTM generated?

Yes, that is correct. A second RTM is generated when the second questionnaire is run.

c. What additional steps does the plan writer need to take, if any?

- i. When running the NASA C&A Questionnaire-Oct 2009 when you get to question 900 select Option 2 and then select Yes to question 905 “Do you want to generate a “System Security Plan” template. All other questions will be no. This will then generate a new System Security Plan (SSP) Rev3. Please do not change the name as it will be confusing as to whether or not you are modifying Rev2 or Rev3 SSP. Rename other supporting documents. Including a reference to Revision 3 in the title will facilitate use of the documents.