

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



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

MAY 18 2010

TO: Distribution

FROM: Deputy Chief Information Officer for IT Security

SUBJECT: Suspension of Certification and Accreditation Activity

This memorandum is for wide distribution. For maximum effectiveness, it is critical that this guidance be distributed to all Information System Security Officials, Information System Owners, Authorizing Officials, managers and operators across all IT domains to include both corporate and mission IT environments, whenever and wherever feasible.

On April 21, 2010, The Office of Management and Budget (OMB) issued memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. The reporting instructions for FY10 significantly change the way federal agencies assess the security posture of their information systems. The memo is clear regarding a shift away from cumbersome and expensive C&A paperwork processes, in favor of a value-driven, risk-based approach to system security.

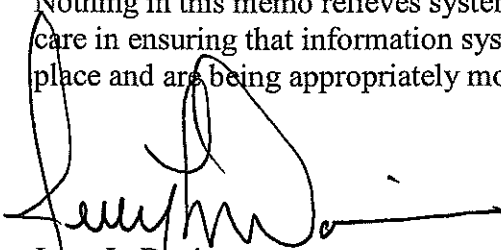
Per M-10-15, NIST recommendations inherently "allow agencies latitude in their application [of security solutions...]. Consequently, the application of NIST guidelines by agencies can result in different security solutions that are equally acceptable and compliant." As such, the ITSD is creating a more streamlined system security authorization process with a focus on continuous monitoring, automated tools, and significant paperwork reduction. These developing processes will eventually enable near real-time risk management and ongoing security authorizations that reflect the true intent of NIST guidance, and fall in line with the objectives of DHS, DOJ, the Whitehouse, recently proposed amendments to federal security legislation, and new OMB mandated tools.

To guide NASA through this strategic transitional period, the IT Security Division (ITSD) within the NASA Office of the Chief Information Officer (OCIO) is issuing the following:

- The OCIO will not require Information System Owners (ISO) to recertify their systems in FY 2010 to satisfy OMB requirements.
- In lieu of C&A activities in FY 2010, AOs must extend current Authorizations to Operate (ATO) for a period not to exceed one year from the date of their system's current ATO expiration, using form NF1740 (see attached sample with appropriate extension conditions).

- Updated ATO expiration dates should be reported to OCIO via normal ITS monthly reporting activities.
- At the discretion of the Authorizing Official (AO), for systems under their cognizant authority, an ATO may still be obtained through existing NASA C&A processes; however, these processes have proven largely ineffective and do not ensure a system's security, or a true understanding of the system's risk posture.
- All new systems (internal and external) will adhere to the current NASA C&A processes to obtain an initial ATO until a more effective security authorization process is established. However, as always intended, the focus of new ATOs should be a near real-time understanding of risk posture, and not the production of paperwork.

Nothing in this memo relieves system owners and operators from exercising due diligence and care in ensuring that information systems under their authority have adequate security controls in place and are being appropriately monitored.



Jerry L. Davis

Enclosure

Distribution:

ITSM

ARC/Mr. Ernest Lopez

DFRC/Mr. Anthony Thomas

GRC/Mr. Les Farkas

GSFC/Mr. Joshua Krage

HQ/Mr. Greg Kerr

JPL/Mr. Jay Brar

JSC/Mr. Ted Dyson

KSC/Mr. Henry Yu

LaRC/Mr. Kendall Freeman

MSFC/Mr. David Black

NSSC/Mr. Dave Epperson

SSC/Mr. Monti Muhsin

Center CIOs

ARC/J. Williams (Acting)

DFRC/R. Binkley

GRC/S. Pillay

GSFC/A. Gardner

HQ/K. Carter

JPL/J. Rinaldi

JSC/L. Sweet

KSC/M. Bolger

LaRC/C. Mangum

MSFC/J. Pettus

NSSC/B. O'Dell

SSC/D. Cottrell

Mission Directorates

Aeronautics Research/P. Milstead

Exploration Systems/B. Hamilton

Science/J. Bredekamp

Space Operations/S. Goodwin



National
Aeronautics and
Space
Administration

IT System Authorization to Operate (ATO)

TO: <SYSTEM OWNER NAME>, Information System Owner

FROM: <AUTHORIZING OFFICIAL NAME>, Authorizing Official

SUBJECT: Security authorization Decision for <NASA SYSTEM NAME>

After reviewing the results of the security assessment of <NASA System Name> and its constituent system-level components, managed by HQ, and the supporting evidence provided in the associated security authorization package, I have determined that the risk to Agency operations, Agency assets, or individuals resulting from the operation of the information system is FULLY ACCEPTABLE.

Accordingly, I am issuing AN ATO WITHOUT ANY SIGNIFICANT RESTRICTIONS OR LIMITATIONS. This security authorization is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system.

The security authorization of this information system will remain in effect as long as: (i) the required security status reports for the system are submitted to this office once every year (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) the system has not exceeded the maximum allowable time period between security authorizations in accordance with Federal or Agency policy.

A copy of this form with all supporting security assessment and authorization documentation must be retained in accordance with the Agency's record retention schedule, as well as posted in the NASA System Security Plan Repository.

Conditions to obtain an ATO are shown below or on a separate document.

CONDITIONS

Per Agency OCIO guidance, this document extends the current authorization to operate (ATO) one year from the date of expiration. It is the expectation of the authorizing official that the system owner will continue to practice due diligence in ensuring the security posture of the information system. This ATO will expire <Insert Current Expiration Date + 1 Year>.

<Authorizing Official Name>

AUTHORIZING OFFICIAL NAME

<Authorizing Official Title>

TITLE

HQ

ORG CODE

CENTER

SIGNATURE - DATE