



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

TO: Distribution

FROM: Deputy CIO for IT Security

SUBJECT: Certification and Accreditation Direction for FY09

In an effort to standardize the methodology used to conduct certification and accreditation (C&A) activities at NASA, align the current C&A process with the latest revision of the National Institute of Standards and Technology (NIST) Special Publication 800-37r1 *Guide for Security Authorization of Federal Information Systems: A Lifecycle Approach*¹ and ensure security controls are consistently implemented throughout the Agency, the OCIO plans to revise its process for conducting C&As beginning in fiscal year (FY) 2009.

C&A Program Review

Immediately after completion of the C&A activities conducted in FY07, the IT Security Program Management Office (ITS PMO) within the Office of the Chief Information Officer (OCIO) conducted a review of the C&A program. This review included a random analysis of C&A documentation, the C&A budget formulation and execution process and the manner in which C&A activities had been executed. The ITS PMO found that using multiple vendors to perform C&A of Agency systems and applications in FY07 led to different C&A approaches, which ultimately resulted in inconsistent results of the independent certifications. The ITS PMO found that the C&A documentation had not been consistently developed and that gaps in the process could expose systems and applications to unnecessary risks. The review also discovered that the process for C&A scheduling and budget formulation and execution should reside with the system and application owners and not with the OCIO.

New Certification and Accreditation Vehicle

It is the decision of the Agency to enter into a contractual agreement with the US Treasury Department's Bureau of Public Debt (BPD) as the sole Certification Agent for future C&A efforts. The C&A services provided by BPD will ensure that the Agency employs a consistent, cost effective and robust C&A process.

¹ The ITS PMO understands that this is a draft document. <http://csrc.nist.gov/publications/drafts/800-37-Rev1/SP800-37-rev1-IPD.pdf>

Responsibilities

It shall be the responsibility of the ITS PMO to serve as the contract sponsor, covering the cost of any contract management fees and managing the general provisions of the contract. It shall be the responsibility of system and application owners to identify systems and applications requiring C&A, budget for C&A and schedule the C&A activity using only the BPD as the Certification Agent once the services is made available. System and application owners will also ensure that payment for C&A activities are made to BPD at the completion of the C&A activity and in accordance with the terms and conditions of the Memorandum of Agreement (MOA). It shall be the responsibility of BPD to serve as the Certification Agent for all Agency systems and applications, to include contractor systems and applications as required by the Federal Information Security Management Act (FISMA). BPD shall execute the C&A process in accordance with federal guidelines and requirements.

New C&A Vehicle Timeline

The new C&A vehicle is expected to be available near the end of Q1 FY09. Until the new C&A vehicle is in place, system and application owners will be required to use the existing C&A vehicle. Once the BPD vehicle is available, the current vehicle (SecureInfo) will be sunset and terminated. System and application owners shall not acquire or retain any C&A vendor outside what is provided by the ITS PMO.

Estimated Certification Costs

BPD has provided the following Rough Order of Magnitude (ROM) for C&A activities:

Low Application - \$37,000

A minor application residing on a general support system (C&A'd separately) that uses SQL server. No external access. Total users < 50.

Moderate Application - \$54,000

A moderate impact application residing on a general support system (C&A'd separately) with Internet access. The system is primarily mainframe with some distributed Windows based components. Total users ~ 100.

Moderate GSS - \$60,000

A moderate GSS comprised of LANs connected together through the use of high-speed communication lines, switches, and routers allowing users to share network resources.

System is comprised of 30 centrally located Windows and Redhat ES4 servers, hardware and software primarily in one geographical region. Includes two (2) remote sites. The WAN network hardware is comprised of switches, routers, firewalls, and intrusion detection systems (IDS). Support systems include servers, Windows XP and Vista workstations, laptops, printers, and scanners. Total users ~ 300.

High Application - \$80,000

A high impact major application also consisting of segregated dedicated infrastructure components. Application is Internet accessible. Comprised of 15 Windows and Redhat servers, Windows XP and Vista workstations, laptops, printers, scanners, and other peripheral components. Total users ~ 600 with most being remote.

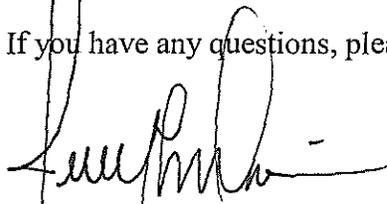
Precise costs and flexibilities will vary depending on specific system complexities, state of existing documentation, and condition and extent of common controls.

C&A Schedules

In order to ensure that C&A is not a one-time process, all systems must be reaccredited at least once every three years or when significant changes to the system affect the system's security. Additionally, all common controls must be certified every year. With the majority of systems being certified in 2007, there is a surge of C&As scheduled for FY 2010. The attached spreadsheet, as reported through the ITS-161 data call, lists the number of C&As (low, moderate and high) scheduled for each Center.

In an effort to plan and budget for upcoming C&A activities it is necessary to project as accurately as possible the timeframe and number of systems requiring C&A over the next three fiscal years (FY-09 through FY-11). In addition, in order to facilitate a more even distribution of system certifications, the OCIO is requesting that each Center review the number of certifications for FY 2010 and distribute them between FY 2009 and FY 2010. Centers are required to submit a revised certification schedule to OCIO identifying a timeline for system certifications over the next three fiscal years using the attached spreadsheet. It is also requested that new systems or existing systems expecting significant changes be considered in this timeline as well.

If you have any questions, please contact Teresa Fryer at Teresa.Fryer-1@nasa.gov.



Jerry L. Davis

DISTRIBUTION:

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

Center CAOs:

ARC/Steve Hunt
DFRC/Anthony Thomas
GRC/Don Cannatti
GSFC/Kanitra Tyler
HQ/Greg Kerr
JSC/Joreen Lee
KSC/Elaine Brabaw
LaRC/Michael Bray
MSFC/Bob Keasling
SSC/Debra Rushing
NSSC/Dave Epperson