Final Audit Report, “Assessment of NASA’s Certification and Accreditation Process” (Report No. IG-07-035; Assignment No. A-07-009-00)

FISMA requires agencies to report annually on the effectiveness of the agency’s IT security program and requires IGs to perform independent evaluations of their agency’s information security programs and practices. For FY 2007, OMB asked IGs to provide a qualitative assessment of their agency’s process for certifying and accrediting IT systems. OMB and NASA OCIO requested that we provide, as a part of the FY 2007 FISMA compliance review, an early assessment of NASA’s process for certification and accreditation (C&A) of unclassified NASA systems categorized as moderate- and high-risk impact. Overall, we found that OCIO’s policies and procedures for the C&A process for unclassified systems are in compliance with FISMA requirements; however, the quality assurance function of the process could be improved. Specifically, we found inaccuracies and inconsistencies in C&A documentation for 11 of 13 security assessment reports we reviewed. Inaccurate and inconsistent information in the security assessment report reduces the assurance that authorizing officials have the information they need to make a credible, risk-based decision about system accreditation—i.e., whether to authorize operation of an information system. OCIO immediately began taking corrective actions to address our concerns.

We recommended that OCIO (1) provide formal notice to the contractor and the contracting officer of our findings and take them into consideration with regard to the contract performance metric for independent certification; (2) increase oversight of deliverables provided by contractors by ensuring that security assessment reports are reviewed for correctness, completeness, and consistency with established standards; and (3) formally remind system personnel, such as system owners, of the importance of reviewing and verifying the accuracy of security assessment reports. Management concurred with all three recommendations and management’s comments were responsive. All three recommendations will be closed upon completion and verification of management’s corrective action.

The memorandum contains NASA Information Technology/Internal Systems Data that is not routinely released under the Freedom of Information Act (FOIA). To submit a FOIA request, see the online guide.