IT Security Certification and Accreditation Process

EXECUTIVE SUMMARY

An Office of Inspector General (OIG) contractor (ECS) evaluated the ACTS Plus and EFOIA applications as part of the OIG's fiscal year 2005 review under the Federal Information Security Management Act (FISMA). These applications were chosen for review because they had been certified and accredited (C&A) this year.

The Office of Management and Budget (OMB) has asked agency Inspector Generals to assess their agency's certification and accreditation process. Based on our review of two Commission systems, we identified several needed improvements in the Commission's C&A process. These concerned the independence of the certification agent, certifying and accrediting the general infrastructure support system (GSS), and improvements to the evaluation process and tracking of Plans of Action and Milestones (POA&Ms).

ECS briefed Commission management on its detailed findings and recommendations. Management promptly began to consider appropriate corrective measures as a result of the identified findings.

OBJECTIVES AND SCOPE

Our objective was to determine if the C&A process used by the Commission met FISMA requirements and OMB and National Institute of Standards and Technology (NIST) standards.

During the review, the contractor interviewed Commission staff, reviewed the applications' security and certification documentation, and analyzed the extent of compliance with applicable standards. ACTS Plus and EFOIA were the sample.

The audit was performed in accordance with generally accepted government auditing standards between July and September, 2005.

BACKGROUND

Accreditation is the official management decision given by a senior agency official to authorize operation of an IT system. It involves explicitly accepting the risk to agency operations, assets, or individuals based on the implementation of an agreed-upon set of security controls.

The supporting evidence needed for security accreditation is developed through a detailed security review of the IT system, referred to as security certification. Certification determines the extent to which controls are implemented correctly, operating as intended, and meet the system security requirements. Certification and accreditation of major IT systems are required by FISMA, and are performed under standards issued by OMB and NIST.

AUDIT RESULTS

We found that security certification and accreditation at the Commission needed to be improved and brought into compliance with OMB and NIST standards, particularly regarding the independence of the certification agent. In addition, the certification of ACTS Plus and EFOIA depended on the certification of the general infrastructure support system (GSS), which had not yet occurred. The processes for the security test and evaluation (ST&E) and the Plans of Action and Milestones (POA&Ms) also needed improvement.

The contractor prepared a detailed report containing its findings and recommendations. Because of the sensitivity of the detailed report, we have decided to issue this public report summarizing the results of our review.