Security Certification and Accreditation of ACTS Plus

EXECUTIVE SUMMARY

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

ECS briefed Commission management on its detailed findings and recommendations. The review found several risk areas in ACTS Plus, including the process for performing the certification and accreditation, contingency planning, and security plans.

Commission management promptly began to consider appropriate corrective measures as a result of the review.

OBJECTIVES AND SCOPE

Our objectives were to determine if the ACTS Plus application met the necessary security requirements prescribed by FISMA and described in Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) standards.

During the review, the contractor interviewed Commission staff, reviewed relevant documentation, and performed visual inspections. The contractor used the information gathered to identify risks to ACTS Plus. It calculated scores to identify the risk level (i.e., high, medium, low) for a number of information technology (IT) areas. The contractor then identified possible solutions to eliminate or mitigate those risks.

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

BACKGROUND

ACTS Plus is a major application that is owned by the Commission's Office of Investor Education and Assistance (OIEA) and maintained by the Office of Information Technology (OIT). ACTS Plus is a web-based application that is used to track investor correspondence with the Commission.

As the system owner, OIEA is responsible for following the IT management and security policies issued by OIT, as well as related statutes and government-wide regulations. OIT provides software development, hardware, and technical assistance to OIEA to help it carry out its IT management functions. OIT also coordinated and implemented the certification and accreditation of ACTS Plus during fiscal year 2005 as required by OMB Circular A-130.

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.

AUDIT RESULTS

We found that security certification and accreditation at the Commission needs 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 depended on the certification of the general infrastructure support system (GSS), which had not yet occurred.

We identified several deficiencies within the ACTS Plus application, including system contingency and security plans. 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.