# M E M O R A N D U M

September 30, 2005

**To:** Corey Booth
Kenneth Fogash

**From:** Walter Stachnik

**Re:** Security Certification and Accreditation of EFOIA (Audit No. 410)

Attached is the public audit report (No. 410) of the EFOIA certification and accreditation. The review was performed by ECS under a contract with our Office. The non-public technical report will be sent separately by email. The detailed recommendations from the non-public technical report will be tracked in the Audit Recommendation Tracking System.

We would appreciate receiving any additional comments you have concerning this audit and the report. In particular, we would like to know whether you found the audit useful. We also welcome any suggestions from you concerning how we could improve future audits.

The courtesy and cooperation of you and your staff during this audit are appreciated.

Attachment

cc: Chrisan Herrod
Peter Uhlmann
Barbara Stance
James McConnell
Dan Lisewski
Darlene Pryor
Richard Hillman
Celia Winter

# Security Certification and Accreditation of EFOIA

## EXECUTIVE SUMMARY

An Office of Inspector General (OIG) contractor (ECS) evaluated the EFOIA application as part of the OIG's fiscal year 2005 review under the Federal Information Security Management Act (FISMA). EFOIA 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 EFOIA, including the process for performing the certification and accreditation, contingency testing and training, and server room controls.

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 EFOIA 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 evaluated and observed physical controls. The contractor used the information gathered to identify risk levels in EFOIA (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

EFOI is a major application used by the Office of Filing and Information Services (OFIS) to process Freedom of Information Act (FOIA) and Privacy Act (PA) requests from individuals and businesses. The application is actually a commercial-off-the-shelf (COTS) product called FOIAXpress developed by AINS, Inc. FOIAXpress is used by several federal agencies in addition to the Commission.

EFOIA is a web-based application that electronically creates, stores, retrieves, redacts, and prints documents for delivery to FOIA requesters. It also keeps track of FOIA processing statistics and fees in addition to generating reports on the number, types, and nature of FOIA requests processed, as required by the Department of Justice. EFOIA is maintained by the Office of Information Technology (OIT), and resides on an application server in the Commission's data center.

As the system owner, OFIS 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. OFIS has also contracted with AINS for application support in troubleshooting EFOIA problems.

OIT coordinated and implemented the certification and accreditation of EFOIA 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 EFOIA depended on the certification of the general infrastructure support system (GSS), which had not yet occurred.

We identified several deficiencies within the EFOIA application, including contingency testing and training, and security room controls. 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.