INFORMATION TECHNOLOGY MANAGEMENT IN ENFORCEMENT

EXECUTIVE SUMMARY

We found that the Division of Enforcement's (Enforcement or the Division) information technology (IT) management was generally adequate. However, the Division needs to issue additional guidance to ensure a sound IT program. During our review, the Division and the Office of Administrative Services (OAS) developed procedures for preventing and resolving physical security incidents at the Division's forensics lab.

To enhance the Division's IT management, we are recommending that it prepare an IT plan and document its procedures for IT management, major initiatives (such as the document imaging project), and security management.

OBJECTIVES, SCOPE, AND METHODOLOGY

Our audit objective was to evaluate the Division of Enforcement's IT management to determine if it was adequate and in compliance with applicable guidelines. During the review, we analyzed relevant IT documentation, interviewed Division, OAS and Office of Information Technology (OIT) staff, and observed the Division's IT operations. The specific areas of review were:

- General IT management;
- IT security management;
- Staff IT training; and
- IT policies, standards and guidelines.

We used selected best practices and standard IT controls (Control Objectives for Information and related Technology or COBIT) to perform this review.

We conducted this performance audit from September 2005 to August 2006 in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

The Office of Information Technology has overall responsibility for Commission IT management. OIT's duties include application development, infrastructure operations and engineering, user support, IT program management, capital planning, security, and enterprise architecture.

Over time, the program offices have gradually assumed significant IT responsibilities, staff, and funding. In particular, the Division of Enforcement has a relatively large IT program, using both employees and contractors.

Enforcement's management views IT as a vital tool in accomplishing its mission. In support of its investigations, Enforcement uses data analysis and mining tools, images evidentiary documents, and extracts files from electronic media.

The Division has established an Office of Technical Services to handle its IT requirements. This Office is composed of three branches: Technical Consulting and Analytical Services, Litigation Support, and IT Forensics.

The Technical Consulting and Analytical Services Branch principally focuses on e-mail, system back-ups, and database issues related to investigations. The Litigation Support Branch images evidentiary records and performs other IT-related duties in support of Enforcement litigation. The IT Forensics Branch's primary function is to extract active and deleted files from electronic media (e.g., hard drives, personal digital assistants).

AUDIT RESULTS

We found that Enforcement IT management was generally adequate. However, the Division needs to issue additional guidance to ensure a sound IT program, including an IT plan and procedures for IT management, major initiatives, and security management. Our detailed findings and recommendations are presented below.

IT PLAN AND PROCEDURES

Enforcement has not yet prepared a formal IT plan, since its Office of Technical Services is relatively new (established in 2005). Also, Enforcement noted that its participation in the Commission's capital planning process acts as a planning tool. However, a formal IT plan would help define Enforcement's current and future IT needs in relation to the Division's strategic goals, and describe the required steps and timeframes for meeting those needs.

Enforcement currently has few written procedures for its IT management, both for day-to-day operations and major initiatives (such as the document imaging project). Written procedures would help Enforcement control and standardize its IT program, especially for forensics and document imaging. The documentation would serve as a reference (particularly for new staff) and help ensure consistent implementation of Enforcement initiatives.

Recommendation A

The Division of Enforcement should prepare a short and long-term IT plan.

Recommendation B

The Division of Enforcement should develop written procedures for its IT management and major IT initiatives.

SECURITY MANAGEMENT

We found that the Division's IT security management can be improved. While the Division has an informal process in place, it does not have written procedures covering its responsibilities for IT security (OIT has responsibility for most Commission IT security). Such procedures would describe Enforcement's approach to security and provide guidance to its IT staff.

In this regard, certain Division security practices need improvement. For example, Enforcement has not defined which staff are authorized to request IT system changes of OIT. Also, Enforcement did not have sufficient back-up staff to support one of its web servers. These conditions could result in inappropriate system changes or web server issues not being resolved timely.

Recommendation C

The Division of Enforcement should develop written procedures describing its IT security management, including system changes and staff support for systems.

FORENSICS LAB PHYSICAL SECURITY

Enforcement indicated that physical security could be an issue for its IT forensics lab. Its access records for the lab showed that it had been entered by an unidentified person who had bypassed Enforcement's normal entry procedures.

The Office of Administrative Services reviewed this issue, and found that an authorized employee in its physical security group had entered the lab. However, OAS did not provide this information to Enforcement. Enforcement is currently trying to get the forensics lab accredited, so it needs information on any possible unauthorized access.

During the audit, we suggested that OAS develop procedures to ensure that (1) its staff follows Enforcement's procedures for access to the IT forensics lab, and (2) it informs Enforcement of the results of its review of physical security incidents at the lab.

Before we issued this report, OAS and Enforcement jointly developed procedures which adequately addressed physical security within the forensics lab. Accordingly, we are not making a recommendation on this issue.