SERO IT MANAGEMENT

EXECUTIVE SUMMARY

An OIG contractor (ECS) reviewed Information Technology (IT) management at the Commission's Southeast Regional Office (SERO). ECS briefed Commission management on its detailed findings and recommendations. The review found several risk areas, including organizational structure for SERO IT management; IT security awareness, practices and procedures; physical building security; and IT security guidance.

OBJECTIVES AND SCOPE

Our objectives were to evaluate the adequacy of SERO's internal controls for IT management and their compliance with applicable guidance. A primary focus of the review was IT security.

During the review, the contractor interviewed Commission staff, reviewed relevant documentation, and performed visual inspections, internal network scans, laptop/workstation analysis, firewall/access control list analysis, and server configuration analysis.

The contractor used the information gathered to identify risks in SERO's IT management. It calculated scores to identify the risk level (*i.e.*, high, medium, low) for a number of IT areas using an algorithm based on IT best practices. 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 November 2004 and January, 2005.

BACKGROUND

The Southeast Regional Office in Miami, FL administers Commission programs in Alabama, Florida, Georgia, Louisiana, Mississippi, North Carolina, Puerto Rico, South Carolina, Tennessee, and the Virgin Islands. It supervises the Atlanta District Office. SERO reports to the Division of Enforcement in Commission headquarters.

In carrying out its responsibilities, SERO relies extensively on information technology to achieve its mission objectives. The Office is ultimately responsible for

the management and security of its IT resources. SERO is accountable for executing the IT management and security policies and regulations developed by the Office of Information Technology (OIT), as well as related statutes and government-wide regulations. OIT also provides technical assistance and hardware to SERO to assist it in carrying out its IT management functions.

AUDIT RESULTS

We found that IT management at SERO needs to be improved, and brought into compliance with Commission guidance. The contractor identified numerous risks, in SERO's IT security awareness, practices, and procedures; building security;[1] organizational structure; and coordination with OIT. In addition, Commission security guidance can be enhanced.

The contractor identified many similar risks in an earlier review at the Northeast Regional Office (Audit No. 392). The actions being taken by OIT to address the risks identified at NERO will also address many of the risks identified at SERO.

Recommendation A

The Southeast Regional Office should take corrective actions, in coordination with the Office of Administrative Services and the Office of Information Technology where necessary, on the identified risks at SERO for its area of responsibility.

Recommendation B

The Office of Information Technology should take corrective actions on the identified risks at SERO for its area of responsibility.

[1] The Office of Administrative Services (OAS) has oversight responsibility for physical security in regional offices. Since all regional offices are located in private, multi-tenant buildings, the daily physical security of the building is handled by building management. The OAS Security Branch provides advisory services to SEC regional management on physical security matters and the OAS Construction and Real Property Branch negotiates leasehold improvements with the building management to implement recommendations to enhance building security. In reality, however, there is little OAS can do to improve the base building security (e.g., guards not checking IDs in the lobby).