NERO IT MANAGEMENT

EXECUTIVE SUMMARY

An OIG contractor (ECS) reviewed Information Technology (IT) management at the Commission's Northeastern Regional Office (NERO). The review was a pilot for future IT management reviews at other Commission field offices.

ECS briefed Commission management on its detailed findings and recommendations. The review found several risk areas, including organizational structure for NERO IT management; IT security awareness, practices and procedures; physical building security; and IT security guidance.

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

OBJECTIVES AND SCOPE

Our objectives were to evaluate the adequacy of NERO'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 and external network scans, laptop/workstation analysis, firewall/access control list analysis, and server configuration analysis.

The contractor used the information gathered to identify risks in NERO'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 July and November, 2004.

BACKGROUND

The Northeast Regional Office in New York City administers Commission programs in Connecticut, Delaware, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, Vermont, Virginia, West Virginia,

and the District of Columbia. It supervises the Boston and Philadelphia District Offices. NERO reports to the Division of Enforcement in Commission headquarters.

In carrying out its responsibilities, NERO relies extensively on information technology to achieve its mission objectives. The Office is ultimately responsible for the management and security of its IT resources. NERO 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 NERO to assist it in carrying out its IT management functions.

AUDIT RESULTS

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

NERO, OIT, the Office of Administrative Services (OAS), and the Office of Executive Director responded to ECS's briefing by outlining several steps they are taking, or have taken, to improve IT management at NERO. We commend them for their prompt actions on the audit findings.

In their responses, these offices explained why they do not plan action on some of the identified findings and recommendations. In some cases, possible corrective actions would be cost prohibitive; would reduce needed functionality; involve relatively low risk or low priority areas; or would duplicate actions being taken on other outstanding audit recommendations.

In general, the approach being taken by these offices to improve NERO IT management appears reasonable. We are recommending that they complete their proposed actions on the identified findings.

Recommendation A

The Northeast Regional Office should take corrective actions as planned, in coordination with the Office of Administrative Services where necessary, on the identified risks at NERO for its area of responsibility.

Recommendation B

The Office of Information Technology should take corrective actions as planned on the identified risks at NERO 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).