

DOE F 1325.8
(8-89)
EFG (07-90)

United States Government

Department of Energy

Memorandum

DATE: September 18, 2007
REPLY TO: IG-34 (A07TG036)
SUBJECT: Evaluation of "The Federal Energy Regulatory Commission's Cyber Security Program-2007"
TO: Chairman, Federal Energy Regulatory Commission

Audit Report No.: OAS-L-07-23

The purpose of this report is to inform you of the results of our evaluation of the Federal Energy Regulatory Commission's (Commission) cyber security program. The evaluation was initiated in May 2007, and our fieldwork was conducted through September 2007. Our methodology is described in the attachment to this report.

INTRODUCTION AND OBJECTIVE

The Commission reports that it is constantly improving the stability, reliability, and security of its information technology (IT) infrastructure and data repositories to help achieve their mission to regulate and oversee energy industries in the economic, environmental, and safety interests of the American public. To accomplish this, the Commission estimated that, in Fiscal Year 2007, it spent almost \$1 million to protect its \$ 26.1 million IT investment from cyber-related threats.

As required by the *Federal Information Security Management Act (FISMA)* and the Office of Management and Budget (OMB) implementing guidance, the Office of Inspector General performed an annual independent evaluation of the Commission's cyber security program. This evaluation is designed to assess the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with FISMA requirements.

CONCLUSIONS AND OBSERVATIONS

Overall, we continued to note improvements in the Commission's cyber security program. In the past year the Commission had taken several actions to strengthen its cyber security program. In particular, it:

- Strengthened password management and corrected prior year problems concerning the use of default, blank, or easily guessed passwords;
- Corrected previously reported issues and updated procedures relating to identifying and promptly disabling unused network accounts;

- Implemented a more robust cyber security self-assessment process and corrected prior year problems in this area; and,
- In response to OMB requirements, developed policies and procedures for protecting personally identifiable information.

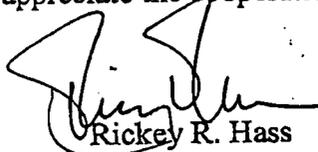
During our current evaluation, we noted an issue related to the completion of risk management activities and security planning for a major financial processing system, the Management Administrative and Payroll System (MAPS). The Commission considers this application critical to its operations and uses it to provide human resources services such as payroll, benefits, time and labor functions, as well as financial functions, including general ledger, accounts receivables, and purchasing. Although MAPS underwent a significant software upgrade in 2005, officials did not initiate action until early 2007 to begin a required reaccreditation of the system. Because of the nature of the software upgrade, significant changes occurred both in the manner in which data was processed and how it was transmitted – a situation that could have potentially introduced security vulnerabilities or increased the risk associated with system operation.

In response to our query regarding MAPS, Commission officials indicated that they had started a comprehensive certification process in January 2007, and have completed a number of important parts of the effort. An asset categorization statement had been developed, a privacy impact assessment completed, and a self assessment – including a contingency plan and configuration plan review – and a security review have been performed. Two remaining items, the risk assessment and system security plan, are expected to be completed by September 30, 2007.

SUGGESTED ACTION

We suggest that the Executive Director ensure that the ongoing risk assessment and re-certification of the MAPS system fully consider the risk posed by the software upgrade and modify system controls, if necessary.

Since no formal recommendations are being made in this letter report, a formal response is not required. We appreciate the cooperation of your staff throughout the audit.



Rickey R. Hass

Assistant Inspector General
for Financial, Technology, and Corporate Audits
Office of Audit Services
Office of Inspector General

Attachment

cc: Executive Director, FERC
Chief of Staff, DOE

Attachment

SCOPE AND METHODOLOGY

SCOPE AND METHODOLOGY

The evaluation was performed between May and September 2007 at the Federal Energy Regulatory Commission (Commission) Headquarters in Washington, DC. Specifically, we performed an evaluation of the Commission's Fiscal Year 2007 unclassified cyber security program. The evaluation included a review of general and application controls in areas such as entity-wide security planning, access controls, application software development, change controls, segregation of duties and service continuity. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls.

To evaluate the adequacy and effectiveness of the Commission's information security policies and practices, we:

- Reviewed the Commission's overall cyber security program to evaluate the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of the *Federal Information Security Management Act (FISMA)*;
- Reviewed Federal statutes and guidance applicable to ensuring the effectiveness of information security controls over information resources supporting Federal operations and assets such as FISMA guidance and Circular A-130 Appendix III, and National Institute of Standards and Technology standards and guidance;
- Assessed controls over network operations to determine the effectiveness related to safeguarding information resources from unauthorized internal and external sources;
- Evaluated the Commission in conjunction with its annual audit of the Financial Statements, utilizing work performed by KPMG, LLP (KPMG), the Office of Inspector General's (OIG) contract auditor. KPMG's efforts included analysis and testing of general and application controls for systems as well as vulnerability scanning of networks; and,
- Analyzed OIG reports issued between 2004 and 2006 and reviewed other audits and evaluations performed by Government Accountability Office and the Office of Management and Budget.

We evaluated the Commission's implementation of the *Government Performance and Results Act of 1993* and did not identify any performance measures specific to unclassified cyber security. We did not rely solely on computer-processed data to satisfy our objectives. However, computer assisted audit tools were used to perform probes of various networks and devices. We validated the results of the scans by

confirming the weaknesses disclosed with Commission officials and performed other procedures to satisfy ourselves as to the reliability and competence of the data produced by the tests.

The evaluation was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy our objective. Accordingly, we assessed internal controls regarding the development and implementation of automated systems. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our evaluation.

Commission officials waived the exit conference.