U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Evaluation Report

The Federal Energy Regulatory Commission's Unclassified Cyber Security Program—2005

DOE/IG-0704

October 2005

Department of Energy

Washington, DC 20585

October 6, 2005

MEMORANDUM FOR THE CHAIRMAN, FEDERAL ENERGY REGULATORY COMMISSION

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Federal Energy Regulatory Commission's Unclassified Cyber Security Program - 2005"

BACKGROUND

The Federal Energy Regulatory Commission (Commission) invested over $27 million in information technology related activities in Fiscal Year 2005 to support its mission of regulating the natural gas industry, hydroelectric projects, oil pipelines, and wholesale rates for electricity. As with other Federal organizations, threat of intrusion or damage to the Commission's network and systems continues to grow. The importance of maintaining a strong cyber defense is well demonstrated by a recent series of damaging intrusions and information compromises at both commercial and Federal organizations. The Commission estimates that it spends about $720,000 each year to protect its information technology investment and data from cyber related threats.

In order to develop a comprehensive framework to protect the Government's information, operations, and assets, the Federal Information Security Management Act (FISMA) was passed by Congress and signed into law by the President as part of the Electronic Government Act of 2002. FISMA requires the Office of Inspector General to perform an annual independent evaluation to assess the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of FISMA. As such, this memorandum and the attached report present the FY 2005 results of our evaluation of the Commission.

RESULTS OF EVALUATION

The Commission continues to make significant strides toward improving its unclassified cyber security program. Since our initial evaluation performed in FY 2002, progress has been made in addressing cyber security program management, planning and execution weaknesses. Our current evaluation, however, revealed several problems that have the potential to put the Commission's systems at risk. In particular, we observed that:

- Access controls, through strong password management, had not been properly implemented for a few systems;

- In some instances, software with known security vulnerabilities was not replaced and users were sometimes provided with higher level privileges than they needed to perform their duties; and,

- Not all known cyber security weaknesses were properly identified and/or tracked to resolution.

These problems existed because the Commission had not consistently performed compliance evaluations required by Federal and organization-specific security directives. As a result, the Commission's systems were at risk of disruption of operations, modification or destruction of sensitive data or programs, or theft or improper disclosure of confidential business information.

During the last several years, the Commission's Office of Chief Information Officer has strengthened cyber security related policies and procedures. In addition, the Commission had completed disaster recovery testing on all major applications and its general support system. These actions are promising, and if fully implemented and maintained, should improve cyber security throughout the organization. Additional actions are necessary, however, to ensure that all of the Commission's critical systems are adequately protected. Accordingly, we have made several recommendations designed to aid management in achieving that goal.

Due to security considerations, information on specific vulnerabilities has been omitted. However, management officials have been provided with detailed information regarding identified vulnerabilities, and in most instances, have taken corrective actions.

MANAGEMENT REACTION

Management generally concurred with our findings and recommendations. Management's comments have been summarized and incorporated in the body of this report where appropriate.

Attachment

cc: Executive Director, FERC
Chief of Staff, DOE
Chief Information Officer, DOE

REPORT ON THE FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBER SECURITY PROGRAM - 2005

TABLE OF CONTENTS

CYBER SECURITY PROGRAM

Program Improvements

During our evaluation, we noted that the Federal Energy Regulatory Commission (Commission) had taken steps to strengthen its cyber security program and implemented countermeasures to reduce network vulnerabilities addressed in our previous evaluation reports. Specifically, the Commission improved the Continuity of Operations Plan and system-specific disaster recovery plans. In addition, a System Development Life Cycle manual was developed and finalized to ensure that all information technology systems support Federal statutes and the Commission's business and strategic objectives.

Risk Management and Control Procedures

Despite a number of improvements in cyber security related policies and procedures, we observed that implementation activities by Commission staff were not always completely effective. Specifically, we identified weaknesses in the areas of system access and configuration controls. We also noted problems with the use and effectiveness of the Plan of Action and Milestones (POA&M) report used to track needed cyber security corrective actions.

Access Controls

We noted that controls over passwords were not always effectively implemented. Passwords used in conjunction with user identifications are a critical element of computer security as they provide the basis for controlling access and establishing accountability by identifying and authenticating users. Our testing revealed that easily guessed, blank, or default passwords existed on a few of the Commission's systems. This condition was contrary to the Commission's policy that passwords must be, among others things, unique, difficult to guess, and a minimum length. When informed of the problems we discovered, site officials took action to resolve many of the identified weaknesses.

Configuration Management

We also observed several configuration management problems that, if exploited, had the potential to permit penetration or unauthorized use of the Commission's systems. Proper application of configuration management ensures that the system in operation is the correct version of

the system and that any changes to be made are reviewed for security implications. Vulnerability scanning disclosed several instances of outdated versions of software with known security vulnerabilities that had not been properly updated. These tests also revealed that improperly configured system servers provided higher-level privileges to users than was necessary for them to perform their duties. As noted in guidance developed by the National Institute of Standards and Technology, individuals should generally be provided with the least privileged access consistent with their assigned duties to help minimize the risk of unauthorized or malicious use.

Plan of Action and Milestones

We also found that cyber security weaknesses were not always adequately identifiable in the POA&M report. During Fiscal Year (FY) 2005, the Commission completed testing on its Continuity of Operations and Disaster Recovery Plans for all major applications and its general support system. As a result of that testing, several weaknesses were identified; however, the POA&M entry describing those findings lacked specific and easily identifiable information. Specifically, 20 weaknesses were consolidated into one entry that referenced "all findings in the disaster recovery test reports." This method does not allow for individual prioritization and allocation of resources, nor does it track system owner accountability as required by Office of Management and Budget guidance.

In addition, we found five other instances where risks noted in the FY 2004 and FY 2005 certification and accreditation (C&A) process were not clearly identifiable in the POA&M. In January 2004, for example, the Commission reported a weakness that a major application lacked a comprehensive disaster recovery plan. Despite its importance, this weakness was assigned a low risk and was grouped together with other weaknesses into a summary entry that described "technical difficulties in meeting recovery points and time objectives" in the POA&M report. Although the weakness had not been corrected as required, full recertification and accreditation (authority to operate) was granted in June 2005, and will remain effective until June 2008. Even though this weakness was aggregated

with others and given a high priority level in the POA&M report, it has remained unresolved since it was identified in January 2004.

Program Implementation

Vulnerabilities existed because compliance evaluations had not been consistently performed as required by Federal and organization-specific security directives. Cyber security personnel had not conducted examinations at regular intervals to determine whether systems were operating according to current security requirements. Also, enforcement of password policy was not always maintained through system audits and monitoring. Commission officials also had not performed compliance evaluations, using manual and automated password auditing and cracking techniques, at regular intervals.

The Commission implemented a number of compensating controls to mitigate the risk of external threats but may not have focused sufficient attention on potential threats by insiders. Specifically, vulnerable systems residing on the internal network were secured behind a firewall that limited access to specific services from external sources. Also, intrusion detection systems that continually monitored both the perimeter and the internal site networks for detection and analysis of intrusions were in place and operational. While generally effective against external threats, these practices do not reduce the insider risk associated with the poor access controls or configuration management problems we observed. Internal users, recognized to be a substantial risk to both Federal and commercial organizations, could take advantage of such weaknesses and damage the Commission's critical systems. To the organization's credit, when we informed site personnel of the problems they took immediate corrective action.

Operational Impacts

Although the Commission's overall cyber security posture had improved, information resources remain vulnerable. The problems we observed placed the Commission at risk of unauthorized access, use, disclosure, destruction, modification, or disruption of its information, operations, and assets. For instance, weak or nonexistent passwords could potentially allow unauthorized access to database and other system servers. Furthermore, continuing to report weaknesses in the current method may hinder the Commission's effort to effectively manage its security problems.

RECOMMENDATIONS

Weaknesses identified during the course of our evaluation were discussed with Commission officials and actions were taken to resolve certain identified problems. To further improve cyber security within the Commission, we recommend that the Chairman require responsible officials to:

1. Conduct compliance evaluations (such as system audits and monitoring) at regular intervals to determine whether systems are operating according to current security requirements, which include (a) the actions of people who operate or use the system and (b) the functionality of technical controls; and,

2. Include identifiable information for each significant cyber security weakness in the POA&M report thereby ensuring the prioritization of corrective actions, establishment of milestones, and allocation of resources to effectively address security weaknesses.

MANAGEMENT REACTION

Management generally concurred with our findings and recommendations and agreed to work toward resolving them using a risk-based approach. Management noted, however, that the scope of non-compliant passwords was limited to non-domain accounts. Management stated that the vast majority of accounts were compliant with Commission policy, but agreed that action should be taken to address reported problems.

Management also indicated that identified risks are tracked in the POA&M and detail on these risks may be included therein or in other supporting documentation. Management pointed out that items are not closed out in the POA&M until all risks pertinent to the items are addressed. While management acknowledged issues described in the report relating to the POA&M, they believed that there were only limited examples where items did not directly reference supporting documentation.

AUDITOR COMMENTS

Management's comments and proposed actions are generally responsive to our findings and recommendations. While we acknowledge that the password weaknesses we found were limited to a few of the Commission's systems, when considered in totality, the issues addressed in our report point to a need to focus on the more timely identification and correction of weaknesses. This need is emphasized by the fact that our testing of the Commission's systems, network devices, workstations and servers, revealed various problems associated with access controls and/or configuration management. As previously noted, any of these weaknesses could have been exploited by malicious users to inflict damage to systems or data important to the Commission and to the regulated community.

We also observed that the POA&M appears to be used appropriately in many instances. It should be noted, however, that the lack of detail we describe in the report involved weaknesses or problems with all five of the Commission's major application systems and the general support system. The omission of details from tracking reports could have affected the Commission's ability to ensure appropriate visibility over these risks.

.

Appendix 1

OBJECTIVE

In accordance with the Federal Information Security Management Act of 2002 (FISMA) requirement that the Office of Inspector General (OIG) perform an annual independent evaluation, our objective was to assess the Federal Energy Regulatory Commission's (Commission) adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of FISMA.

SCOPE

The evaluation was performed between July and September 2005 at the Commission in Washington, DC. Specifically, we performed an evaluation of the Commission's FY 2005 unclassified cyber security program. The evaluation included a review of general and application controls in areas such as entity-wide security planning and management, access controls, application software development and change controls, and service continuity. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls.

METHODOLOGY

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

- 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 (NIST) standards and guidance;

- 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 FISMA;

- 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 OIG's contract auditor. KPMG's efforts included analysis and testing of general and application controls for systems as well as vulnerability scanning and penetration testing of networks; and,

- Analyzed OIG reports issued between 2002 through 2004 and reviewed other audits and evaluations performed by the Government Accountability Office (GAO) and OMB.

We evaluated the Commission's implementation of the *Government Performance and Results Act* related to the establishment of performance measures for 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.

An exit conference was held with Commission officials on October 4, 2005.

RELATED AUDIT REPORTS

- *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements* (GAO/05-552, July 2005). GAO reported that overall, the government is making progress in its implementation of FISMA. However, as reported pervasive weaknesses in the 24 major agencies' information security policies and practices threaten the integrity, confidentiality, and availability of Federal information and information systems. Access controls were not effectively implemented; software change controls were not always in place; segregation of duties was not consistently implemented; continuity of operations planning was often inadequate; and security programs were not fully implemented at the agencies. These weaknesses exist primarily because agencies have not yet fully implemented strong information security management programs and put federal operations and assets at risk of fraud, misuse, and destruction. In addition, they place financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

- *Evaluation Report: The Department's Unclassified Cyber Security Program 2004* (DOE/IG-0662, September 2004). While actions taken to improve its unclassified cyber security program are commendable, problems continue to exist in the Department of Energy's classified cyber security program that, if uncorrected, could expose critical systems to compromise. As reported, the Department had not completed implementation of a comprehensive risk management program.

- *Evaluation of the Federal Energy Regulatory Commission's Cyber Security Program 2004* (OAS-L-04-21, September 2004). Despite making improvements in its unclassified cyber security program, the Commission had not completed contingency planning, risk management, and certification and accreditation of systems. Although the Commission used the NIST risk assessment methodology as required by FISMA, it had yet to finalize a risk assessment methodology tailored to its needs-a key step in determining current security vulnerabilities within an organization and implementing mitigating controls. Additionally, at the time of the evaluation the Commission had only completely tested one of its five system-level contingency plans. Successful completion of these ongoing initiatives should help correct remaining cyber security problems at the Commission.

- *Audit Report: Management of the Federal Energy Regulatory Commission's Information Technology Program* (DOE/IG-0652, June 2004). The audit disclosed that while action had been initiated to improve the management of its information technology (IT) program, the Commission's critical e-Government development efforts suffered from incomplete project cost estimates, schedule slippages or faced premature obsolescence. The Commission had not prepared an enterprise architecture to integrate business processes and organizational goals

with IT. Without improvement, the Commission risks incurring unnecessary costs for systems that face premature obsolescence because they do not meet user needs or satisfy mission requirements. In the FY 2005 budget request, the Commission included a performance goal to complete an enterprise architecture by October 2004.

- *Evaluation of The Federal Energy Regulatory Commission's Cyber Security Program 2003* (OAS-L-03-21, September 2003). The evaluation of the Commission's unclassified cyber security program reported that significant progress was made in resolving weaknesses reported during the 2002 evaluation. However, plans for maintaining or resuming critical operations in the event of an emergency or disaster had not been completed.

- *Evaluation Report: The Federal Energy Regulatory Commission's Unclassified Cyber Security Program 2002* (DOE/IG-0569, September 2002). The evaluation of the Commission's unclassified cyber security program reported that while a number of protective measures had been implemented, certain critical information systems remained at risk. Cyber protection efforts suffered from program management, planning, and execution weaknesses.

IG Report No. DOE/IG-0704

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Leon Hutton at (202) 586-5798.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost
effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form