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 - 2008

DOE/IG-0802 September 2008

Department of Energy
Washington, DC 20585

September 17, 2008

MEMORANDUM FOR THE CHAIRMAN, FEDERAL ENERGY REGULATORY COMMMISSION

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2008"

BACKGROUND

The Federal Energy Regulatory Commission depends on information technology to support its strategic goals of promoting the development of a strong energy infrastructure, supporting competitive markets, and preventing market manipulation. As with virtually all Government and private sector organizations, the Commission is faced with numerous and increasingly sophisticated attacks on its systems and data. To address this challenge and the continuing threat to its systems, the Commission expects to spend about $5 million in Fiscal Year (FY) 2008 to protect its IT infrastructure and data from cyber security related threats.

The *Federal Information Security Management Act* (FISMA) provides for the management and oversight of information security risks by requiring that organizations design and implement controls to protect Federal information and systems. As required by FISMA, the Office of Inspector General conducts an annual independent evaluation to determine whether the Commission's unclassified cyber security program adequately protects its information systems and data. As such, this memorandum and the attached report present the results of our evaluation for FY 2008.

RESULTS OF EVALUATION

The Commission had taken action to improve cyber security practices and implemented protective measures designed to defend its networks against malicious attackers and other external threats. Our evaluation, however, disclosed that additional actions are needed to reduce the risk of compromise to the Commission's business information systems and data to an acceptable level. Specifically, we observed that:

- Systems were authorized to operate without sufficient testing of the adequacy of mandatory cyber security controls;

- Cyber security incidents were not always handled and reported in accordance with Federal requirements, thereby preventing collection of information necessary for assisting law enforcement or performing trend analysis;

Printed with soy ink on recycled paper

- A number of network accounts had not been terminated as required, a situation that could have enabled terminated individuals to access sensitive information to which they were not entitled or to damage systems;

- Roles and responsibilities for individuals with significant development or cyber security functions had not been properly segregated, providing the opportunity for them to take actions such as introducing unauthorized software and modifying access rights without authority; and,

- Several devices with known software security vulnerabilities were connected to the Commission's network. In certain instances, encryption was not used to protect sensitive data on laptop computers and personal data assistants.

These problems existed because the Commission had not fully developed or implemented all current Federal cyber security requirements. In response to our inquiries, management stated that due to the recent departure of a large number of information technology staff, insufficient attention had been given to ensuring that existing policies and procedures were implemented. FERC management also noted that newer staff was not always made aware of all cyber security requirements. In addition, weaknesses with the Commission's "Plan of Action and Milestone" tracking system prevented it from properly managing the remediation of identified cyber security weaknesses. As a consequence, the Commission's systems were at risk of disruption, modification or destruction of sensitive data or programs, and/or the theft or improper disclosure of sensitive regulatory information.

During the past year, the Commission made progress in improving certain aspects of its cyber security program. For example, a secondary processing location was secured to ensure that critical operations could be recovered and continue in the event of an emergency or disaster. Also, an online service was procured to provide annual cyber security awareness training, thus enabling automated tracking of employee participation and incorporating current Federal cyber security requirements. These actions demonstrate incremental improvements and are the type of actions that, if sustained, should help improve the Commission's cyber security posture. However, additional actions are necessary to ensure that the Commission's systems and information are adequately protected. To that end, we made several recommendations designed to assist in achieving this goal.

Due to security considerations, information on specific vulnerabilities has been omitted from this report. However, management officials have been provided with detailed information regarding identified vulnerabilities, and in certain instances, initiated or completed corrective action.

MANAGEMENT REACTION

Management agreed with the information contained in the report and concurred with each of the specific recommendations. Management stated that measures were being

taken to ensure that the issues highlighted in our report are addressed. Due to security considerations, management's comments have not been included as an attachment to this report.

Attachment

cc: Acting Deputy Secretary, Department of Energy
Executive Director, FERC

EVALUATION REPORT ON THE FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBER SECURITY PROGRAM - 2008

TABLE OF CONTENTS

Unclassified Cyber Security Program

Details of Finding 1

Recommendations and Comments.....7

Appendices

1. Objective, Scope, and Methodology 8

2. Prior Reports 10

Program Improvements

The Federal Energy Regulatory Commission (Commission) had taken several actions to strengthen its cyber security program. Specifically, the Office of the Chief Information Officer made significant progress in continuity of operations planning by securing a secondary processing location to ensure that critical operations could be recovered and continue in the event of an emergency or disaster. In addition, the Commission improved the efficiency of its annual cyber security awareness training by procuring and utilizing an online service available to government agencies. This service enables automated tracking of employee participation and incorporates current Federal cyber security requirements. These activities supplement the Commission's defense-in-depth approach, which utilizes such measures as intrusion detection systems and firewalls to safeguard its networks, systems, and information from malicious individuals attempting to intrude and other external threats.

Risk Management and Security Controls

Despite these improvements, additional effort is needed to ensure that all components necessary to sustain a comprehensive cyber security risk management program are operating effectively. Specifically, we found that systems were authorized to operate without sufficient testing of mandatory cyber security controls. Also, cyber security incidents were not always handled and reported in accordance with Federal requirements. In addition, we identified weaknesses in the areas of access controls, segregation of duties, and configuration management.

Certification and Accreditation

The Commission had certified and accredited its systems; however, it had omitted testing the adequacy of all mandatory cyber security controls – a critical element in the certification and accreditation (C&A) process. Specifically, each of the seven systems we reviewed were certified and accredited without testing for the presence and adequacy of all minimum security controls. Although required by the National Institute of Standards and Technology (NIST) guidance, risk-level appropriate tests of these systems were not completed. As noted by NIST, it is essential that agency officials have complete and accurate information on the security status of their major and general support systems in order to make timely, credible, risk-based decisions on whether to authorize operation of

those systems. Failure to have the necessary information could result in a system being authorized to operate with undetected cyber security weaknesses.

Incident Response Management

Cyber security incidents were not always handled and reported by the Commission in accordance with Federal requirements. NIST guidance requires that agencies implement an incident handling capability that includes preparation, detection and analysis, containment, eradication, recovery, and prompt reporting of incident information to appropriate authorities. To satisfy these requirements, the Commission utilizes the Department of Energy's Computer Incident Advisory Capability (CIAC) to perform cyber security incident handling functions and to forward reports on incidents to law enforcement authorities, where appropriate, and to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) for intrusion trend analysis. CIAC is to be notified of all cyber security incidents, both successful and unsuccessful, that fall into six categories, including compromise/intrusion, web site defacement, malicious code, denial of service, critical infrastructure protection, and unauthorized use. However, prior to our review, the Commission had only been reporting incidents involving personally identifiable information to CIAC. Also, the Commission was not consistently providing monthly negative reports to CIAC, an action required when no incidents are detected. Failure by the Commission to properly handle and promptly report all cyber security incidents jeopardizes the ability of CIAC to collect and forward information necessary to assist law enforcement authorities or enable US-CERT to perform intrusion trend analysis.

Access Controls

Despite Federal direction and Commission procedures, insufficient reviews were performed of network user accounts. The Commission's procedures required that accounts that had been inactive for the past 90 days should be disabled to help prevent unauthorized system access – a requirement consistent with NIST guidance. While the Commission performed a review of user accounts with privileged access to the unclassified network, such as

system administrators, a periodic review of all other network accounts had not been conducted. As a result, we noted that a number of inactive accounts existed on the Commission's network. These accounts could have enabled terminated users or individuals no longer having a valid need to access sensitive information or cause harm and/or damage to Commission systems.

Segregation of Duties

The roles and responsibilities for the developers, database administrators, and security administrators had not been properly segregated on the Commission's network. Consistent with NIST guidance, functions such as systems programming, system management, and network security should be segregated to prevent an individual from having conflicts of interest in responsibilities and duties, or all of the authority or information access necessary to perform fraudulent activities without collusion. However, contrary to this guidance, we observed that 13 application developers and support staff had privileges that, if exploited, could have enabled them to install malicious, untested, or unapproved software on various systems.

Also, the "least privilege" concept had not been enforced to restrict user access for the performance of specified job duties. As noted in NIST guidance, 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. However, we noted that three users had been granted excessive privileges which enabled them to add, remove, and modify not only their own access rights, but also those of other users, without review or approval. In addition, these users also possessed privileges, incompatible with their job duties, to perform various database functions.

Configuration Management

We identified several configuration management problems that, if exploited, had the potential to permit penetration or unauthorized use of the Commission's systems and data. Specifically, servers and communication devices with

known uncorrected software vulnerabilities were connected to the Commission's network. Also, encryption software, specifically required by the Office of Management and Budget (OMB) for protecting sensitive information had not been installed on all laptop computers and personal data assistants assigned to staff. It should be noted that the Commission did acquire a software product during FY 2008 that provides full hard disk encryption on laptop computers, but the installation process had not been completed. In addition, the Commission had still not fully implemented two-factor authentication[1] for remote network access, almost two years after deadlines established by OMB.

Program Implementation

These problems occurred, at least in part, because the Commission had not fully developed or issued policies and procedures that incorporated all current Federal cyber security requirements. Also, security officials did not always ensure the requirements were appropriately implemented. Management, for instance, noted there had been a recent turnover of a large number of information technology team members and as a consequence cyber security operations had not been given adequate attention. In addition, an inadequate Plan of Action and Milestone (POA&M) tracking system prevented the Commission from properly managing the remediation of identified cyber security weaknesses.

Cyber Security Policy and Procedures

Cyber security policy and procedures had not always been developed and issued consistent with current Federal cyber security requirements. For example, the incident response policy and procedures lacked important and detailed steps to be taken in the event of an incident and contained outdated information regarding incident reporting. Key information was omitted, such as identifying CIAC as the entity tasked with tracking incidents and reporting them to external agencies and law enforcement. In another example, while Commission procedures addressed the NIST requirement that the certifying official validate the results of security control testing prior to accreditation, the

[1] Two-factor authentication requires the use of two independent means of establishing a user's identity, such as both a physical device and a password, to gain access to a system.

procedures did not provide details on what controls to test in carrying out the certification process.

Management Attention

Where cyber security policy and procedures did exist, security officials did not always ensure the requirements were appropriately implemented. For instance, security officials acknowledged that, due to the lack of either account auditing tools or familiarity with procedures, a review of user account access had not been conducted according to current Commission requirements. As noted in Commission policy, periodic user account access reviews are essential for ensuring that users who no longer have a valid need to access information systems are denied access to these systems. Management also noted that they had recently lost a number of key cyber security staff and did not devote sufficient attention to ensure proper and full implementation of policies and procedures. They also stated that some newer staff had not been made fully aware of Federal and Commission cyber security requirements.

Plan of Action and Milestones

In addition, problems with the use and effectiveness of the POA&M reports prevented the Commission from adequately indentifying, tracking and monitoring cyber security weaknesses and the status of corrective actions. As noted in NIST guidance, POA&Ms are important for managing an entity's progress towards eliminating gaps between required security controls and those that are actually in place. However, we observed that:

- All currently unresolved findings or security weaknesses were not tracked in the POA&M. For example, although the Commission had identified that it had a problem with devices with known security vulnerabilities being connected to the network; it had not captured this weakness in the POA&M. Consequently, the vulnerability could not be tracked to resolution and was not reported to OMB as required.

- POA&M entries contained insufficient detail or generic information about findings or security weaknesses. Contrary to OMB and NIST

requirements, some entries lacked specific detailed steps or milestones for completing the remediation process. Others provided no information on the cost associated with remediation. Such information is necessary for linking costs to annual cyber security budget requests.

- The POA&M provided no pre-2008 history of prior cyber security weaknesses and the results of remediation activities. Prior history on weaknesses should be included in the POA&M to not only provide information necessary for risk assessment and management purposes but also for use by OMB and other cognizant entities in evaluating the effectiveness of the Commission's cyber security program and use of resources.

It should be noted that in FY 2005, we reported on similar problems regarding the use and effectiveness of the Commission's POA&M report. At that time, the Commission had taken sufficient action to resolve these problems. However, based on the results of our current evaluation, the controls designed to address the issue appear to no longer be completely effective and additional corrective action is necessary.

Operational Impacts

While certain aspects of the Commission's overall cyber security posture had improved, information resources remain more vulnerable than necessary to compromise or attack. Failure to place emphasis on correcting identified weaknesses unnecessarily places the Commission at risk of unauthorized disclosure, destruction, modification, or disruption of its information, operations, and assets. For instance, lost or stolen computer laptops or mobile devices could potentially allow unauthorized access to unencrypted sensitive personal information or data relating to the Commission and its operations. Furthermore, without improvement in its incident response management approach, the Commission will not be able to fully satisfy Federal requirements "…to report all unauthorized system activity or cyber security incidents quickly and accurately " and to certify annually that it has established a process that ensures timely and accurate reporting to the Department, US-CERT, and, where appropriate, law enforcement authorities.

RECOMMENDATIONS

Weaknesses identified during the course of our evaluation were discussed with Commission officials. To the Commission's credit, management took prompt action to correct a number of the weaknesses we identified. They also acknowledged the need to update various policies and guidance and established deadlines for completion of these tasks. However, to further enhance the Commissions cyber security posture, we recommend that the Chairman take action to:

1. Complete corrective actions to address the remaining vulnerabilities identified in this report;

2. Revise and update cyber security policies and procedures, where necessary, to ensure consistency with current Federal cyber security requirements, particularly in the areas of incident response and system C&A;

3. Direct security officials to perform sufficient reviews and take necessary actions to ensure that the cyber security program is performing in accordance with requirements and operating as designed; and,

4. Develop guidance, as necessary, to ensure the POA&M report includes the information necessary to properly identify, track, and monitor all internally and externally identified cyber security weaknesses and remediation activities.

MANAGEMENT REACTION

Management agreed with the information contained within the report and concurred with each of the specific recommendations. The Executive Director provided comments stating that corrective action had been initiated to address the recommendations and strengthen the Commission's overall cyber security posture. In addition, management's comments provided specific timelines for completion of corrective actions.

AUDITOR COMMENTS

Management's comments are responsive to our recommendations.

OBJECTIVE

To determine whether the Federal Regulatory Commission's (Commission) Unclassified Cyber Security Program adequately protected data and information systems.

SCOPE

The evaluation was performed between June and September 2008 at the Commission in Washington, D.C. Specifically, we performed an assessment of the Commission's Unclassified Cyber Security Program. The evaluation included a review of general and application controls in areas such as security management, access controls, configuration management, segregation of duties, and contingency planning. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls.

METHODOLOGY

To accomplish our objective, 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 the *Federal Information Security Management Act* (FISMA), Office of Management and Budget FISMA guidance and Circular A-130 (Appendix III), and National Institute of Standards and Technology standards and guidance;

- Reviewed the Commission's overall cyber security program management, policies, procedures, and practices;

- 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. OIG and KPMG work included analysis and testing of general and application controls for the network and systems and review of the network configuration; and,

- Reviewed reports issued by the OIG and by the Government Accountability Office.

The evaluation was conducted in accordance with generally accepted Government auditing standards for performance audits. Those standards require that we plan and perform the effort to obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusions based on our objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our objective. We assessed significant internal controls and the Commission's implementation of the *Government Performance and Results Act of 1993* and determined that it had established performance measures for unclassified cyber security. Because our evaluation was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our evaluation. We relied on computer processed data sufficient to satisfy certain objectives of the evaluation; we confirmed the validity of such data, where appropriate, by reviewing supporting source documents.

The Commission waived an exit conference.

PRIOR REPORTS

Office of Inspector General Reports

- *Evaluation of The Federal Energy Regulatory Commission's Cyber Security Program-2007* (OAS-L-07-23, September 18, 2007). Overall, we continued to note improvements in the Commission's cyber security program. During our evaluation, we found that a major financial processing system had undergone a significant software upgrade in 2005, but the system had not been recertified and reaccredited for operation. 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 the system upgrade, Commission officials provided evidence that they had started a comprehensive recertification process in January 2007, and had completed a number of important parts of the effort. Since corrective actions were well underway, we did not make any recommendations. However, we suggested that the Executive Director ensure that the ongoing risk assessment and re-certification of the system fully consider the risk posed by the software upgrade and modify system controls, if necessary.

- *Audit Report: Management Controls over the Federal Energy Regulatory Commission's Cyber Security Program - 2006* (OAS-M-06-10, September 2006). The Commission continued to strengthen its cyber security program and had completed action on several issues identified during prior reviews. However, the evaluation disclosed several opportunities to improve the effectiveness and decrease the risk associated with the Commission's cyber security program in the areas of access controls and security assessments. These vulnerabilities existed because the Commission had not ensured that certain aspects of its cyber security program conformed to either Federal or Commission requirements or guidelines. Weaknesses such as the ones we discovered detract from the overall effectiveness of the Commission's cyber security program and potentially expose its information technology resources and data to compromise.

- *Evaluation Report on The Federal Energy Regulatory Commission's Unclassified Cyber Security Program - 2005* (DOE/IG-0704, September 2005). While the Commission continued to make strides toward improving its unclassified cyber security program, our evaluation revealed several problems that have the potential to put the Commission's systems at risk. These problems were found in the areas of access controls, configuration management, and corrective action reviews. 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.

Government Accountability Office Reports

- *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses* (GAO-07-837, July 2007). Almost all major Federal agencies had weaknesses in one or more areas of information security controls. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer resources. In addition, agencies did not always manage the configuration of network devices to prevent unauthorized access and ensure system integrity, such as patching key servers and workstations in a timely manner; assign duties to different individuals or groups so that no one individual had control of all aspects of a process or transaction; or maintain or test continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies had not fully implemented their information security programs. As a result, agencies may not have assurance that controls are in place and operating as intended to protect their information resources, thereby leaving them vulnerable to attack or compromise.

  Nevertheless, Federal agencies continued to report steady progress in implementing certain information security requirements. For Fiscal Year (FY) 2006, agencies generally reported performing various control activities for an increasing percentage of their systems and personnel. However, Inspector Generals at several agencies disagreed with the information the agency reported and identified weaknesses in the processes used to implement these activities. Further, although Office of Management and Budget enhanced its reporting instructions to agencies for preparing FY 2006 FISMA reports, the metrics specified in the instructions do not measure how effectively agencies are performing various activities, and there are no requirements to report on a key activity. As a result, reporting may not adequately reflect the status of agency implementation of required information security policies and procedures.

IG Report No. DOE/IG-0802

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 inspection 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 Judy Garland-Smith (202) 586-7828.

This page intentionally left blank.

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.energy.gov

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