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 - 2009

DOE/IG-0830

October 2009

Department of Energy
Washington, DC 20585

October 29, 2009

MEMORANDUM FOR THE CHAIRMAN, FEDERAL ENERGY REGULATORY COMMISSION

Greg Friedman

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Evaluation Report on the "Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2009"

BACKGROUND

The Federal Energy Regulatory Commission (Commission) is tasked with regulating and overseeing important aspects of the U.S. energy industry. To help meet its goals and objectives, the Commission utilizes varying types of information technology resources. However, reliance on information technology, while certainly beneficial, often creates or increases various risks. For example, cyber attacks against government systems and assets continue to grow in frequency and have become increasingly sophisticated. The Commission expects to spend over $4 million during Fiscal Year (FY) 2009 to help mitigate this increasing threat and to secure its information technology assets.

The *Federal Information Security Management Act of 2002* (FISMA) provides direction to agencies on the management and oversight of information security risks, including design and implementation of 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 cyber security program adequately protects its information systems and data. This memorandum and the attached report present the results of our evaluation for FY 2009.

RESULTS OF AUDIT

In response to the deficiencies identified during our FY 2008 review, the Commission had taken steps to improve its cyber security program. However, our current evaluation revealed that additional actions are necessary to help ensure the Commission's network, systems and data are adequately protected against increasingly sophisticated cyber security attacks. Specifically, we found that:

- Policies and procedures for handling and protecting certain types of sensitive data, including proprietary, privileged, and non-public information stored in or processed by the Commission's information systems had not been developed and implemented;

- Even though we had identified it as an issue over the past several years, the Commission's process for identifying, tracking, and correcting identified security weaknesses still did not fully adhere to Federal requirements and corrective actions were not always completed in a timely manner; and,

- Access controls had not been fully implemented for the Commission's major information systems, all of which potentially contained sensitive data. For example, weaknesses were identified that could have permitted an individual with malicious intent to gain unauthorized access to systems and data.

These problems occurred, at least in part, because the Commission had not developed policies and procedures to address all Federal requirements pertaining to information security. In addition, officials had not always effectively implemented existing policy and/or corrected previously observed weaknesses. For instance, policies and procedures were not sufficient to protect all types of sensitive information. In addition, the Commission's Plan of Action and Milestones process for addressing cyber security weaknesses did not include all information necessary to ensure effectiveness. Absent improvements, the risk to the agency's information systems and data remains higher than necessary.

During the past year, the Commission had made progress in improving the cyber security posture of its computing environment. For example, improvements were made to the process for identifying, handling, and reporting cyber security incidents. In addition, two-factor authentication was implemented for remote access to Commission systems and encryption software was installed to protect information on laptops. While these efforts are noteworthy, our report includes recommendations for additional actions which, when fully implemented, should help strengthen the Commission's cyber security posture.

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 concurred with the report's recommendations and disclosed that it had initiated or already completed actions to address weaknesses identified in our report. Management's comments are included in their entirety in Appendix 3.

Attachment

cc: Deputy Secretary
Executive Director, Federal Energy Regulatory Commission

EVALUATION REPORT ON THE FEDERAL ENERGY REGULATORY COMMISSION'S UNLCASSIFIED CYBER SECURITY PROGRAM - 2009

TABLE OF CONTENTS

Commission's Unclassified Cyber Security Program

Appendices

Commission's Unclassified Cyber Security Program

Program Improvements

During the past year, the Federal Energy Regulatory Commission (Commission) had made significant progress in improving its cyber security program. Specifically, corrective actions had been taken to address four of the five findings identified during our Fiscal Year (FY) 2008 Federal Information Security Management Act (FISMA) evaluation. Our current review revealed improvements in the areas of incident response, access controls, segregation of duties, certification and accreditation, and configuration management. Specifically, the Commission:

- Established policies and procedures for the identification, handling and reporting of security incidents; including performing negative reporting and notifying the Department of Energy's Cyber Incident Response Capability of all incidents that require reporting;
- Developed and implemented policies for ensuring appropriate segregation of duties over its Management Administrative and Payroll System;
- Implemented the use of two-factor authentication for remote access to its network and installed encryption software on all laptop computers; and,
- Had taken steps to improve certain aspects of its Plan of Action and Milestones (POA&M) process.

Risk Management and Security Controls

Despite the various improvements noted, additional action is needed to help ensure the Commission's cyber security program adequately protects its systems and data against internal and external threats. Specifically, areas of concern identified during our FY 2009 evaluation include protection of sensitive information, management of the POA&M process, and the improvement of access controls.

Protection of Sensitive Information

Over the past year, the Commission acquired encryption software for laptops used at its Headquarters and field locations and developed policies and procedures for handling and protecting personally identifiable information (PII). These are positive actions and should, if properly administered, help protect PII. Our current evaluation, however, revealed that policies were not in place to address the protection of other types of sensitive information developed and/or handled by the Commission. Specifically, we determined that not only had the Commission not developed policy detailing how certain types of information such as proprietary, privileged, and non-public information should be protected, it was also unable to document what types of information were to be considered sensitive. Without descriptive policies, users may be unable to determine what types of information require protection and how such information should be secured.

The National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, requires agencies to ensure controls are in place for the protection of sensitive information, especially data sent by email or transmitted off-site. Our review disclosed, however, that absent policies describing what types of information were considered sensitive, procedures or technologies – such as encryption – were not in place for protecting all types of sensitive information maintained in the Commission's three major systems or the General Support System. Each of these systems potentially contained sensitive information and were rated as a "moderate" risk level according to NIST Federal Information Processing Standard 199.

Plan of Action and Milestones

Although numerous steps had been taken to improve POA&M management, the Commission's process for identifying, tracking, and correcting cyber security weaknesses still did not fully satisfy Federal information security requirements. We had previously reported on deficiencies in the POA&M process, including instances of insufficient detail in the POA&Ms, in our *Evaluation Report on the Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2008* (DOE-IG-0802, September 2008). However, our current review disclosed that Office of Management and Budget (OMB) and NIST direction was not fully adhered to when the Commission recently updated its POA&M process. In particular:

- Contrary to NIST and OMB direction, POA&Ms provided by the Commission did not contain required information such as the severity of identified weaknesses; estimated funding resources required to resolve deficiencies; and, detailed milestones and related completion dates for supporting overall POA&M weaknesses. As noted in our prior year findings, detailed information such as this is necessary for management to adequately assess progress, prioritize remediation activities, tie remediation to budgeting and capital planning and investment activities, and help ensure timely completion of POA&M activities.

- POA&Ms contained generic information or insufficient detail regarding actions necessary for remediation. In particular, POA&M items did not contain detailed milestones supporting the mitigation of noted deficiencies. For example, even though the target completion date for one entry had slipped by 22 months because the level of effort required to complete this activity was greater than anticipated, no milestones were added to the POA&M to assist in tracking progress. Furthermore, officials provided no estimates on the amount of funding expected to complete the task. Likewise, we noted that none of the 73 open POA&Ms items contained specific milestones to aid in tracking progress to completion. To their credit, officials had instituted a new database to assist management with tracking the status of corrective actions.

- A number of POA&M items were closed even though remediation activities had not been completed. For instance, between May and December 2008, the Commission closed most POA&M items related to the need to update each of its system security plans to include all required NIST SP 800-53 controls. However, our review of the security plans noted that they had not been appropriately updated even though the action was reported as completed.

As previously noted, the Commission did take steps to improve the POA&M process over the past year. However, to help ensure information needed to adequately manage identified weaknesses within the organization's cyber security program is accessible, additional action is necessary to enhance the Commission's ability to correct identified weaknesses in a timely manner.

Access Controls

We determined that the Commission had not fully implemented effective access controls over its major information systems, all of which potentially contain sensitive data. During our prior year evaluation, we identified weaknesses in the area of network account management. Although officials had taken certain actions to remedy this issue, we continued to note that a periodic review of user accounts and related access privileges had not been conducted. While management's response to the prior year finding indicated that this review was to have taken place around October 2008, the planned review still had not been completed as of the time of our review. Periodic reviews are important to ensure access is terminated for those individuals who no longer have a valid need to access sensitive information or could cause harm and/or damage to Commission systems.

In addition, we identified issues related to account modification monitoring. In particular, even though required by Federal regulations, the Commission had not deployed an automated mechanism to audit account modifications for the General Support System and notify appropriate individuals. Specifically, access change authorizations were not logged, thereby eliminating the ability of management to review them for appropriateness. We also found that while a corrective action item was included in the POA&M to apply account management policies to all Commission systems that require user authentication, the recently developed Account Management Policy did not address review, audit, and continuous monitoring of account modifications and change access authorizations. Absent controls such as these, an authorized individual may be able to gain or elevate levels of access to the Commission's systems without detection.

Cyber Security Program Implementation

The problems identified occurred, at least in part, because the Commission had not developed policies and procedures to address all Federal requirements pertaining to information security. When sufficient policies did exist, officials had not always ensured that they were implemented.

Policies and Procedures

Policies and procedures consistent with Federal cyber security requirements had not always been developed by the Commission. For instance, officials had not ensured that all requirements for the protection of sensitive information had been incorporated into agency policy and implemented by the Commission. As previously noted, while the Commission had developed policies related to the protection of PII, policies were not adequate to ensure protection of other sensitive data used by the agency. In addition, the recently developed Account Management Policy did not address the review, audit, or continuous monitoring of account modifications and change access authorizations. We also found that because Commission officials were unfamiliar with certain Federal requirements, procedures for developing and maintaining POA&Ms were not completely effective.

Program Management

Officials had not always effectively implemented existing policy and/or corrected all of the previously observed weaknesses. Specifically, we found that not only were new areas of concern identified during our current review, but management had not adequately addressed previously identified weaknesses. For instance, the Commission had not taken corrective actions to address one finding issued during our FY 2008 review related to access controls. In addition, although certain steps were taken related to identified POA&M weaknesses, we noted additional issues during our current evaluation. The identified weaknesses were brought to management's attention during our previous review; however, action had not been taken to close all of the findings.

Systems and Data at Risk

The Commission had made significant progress during the past year in improving its overall cyber security program; however, additional effort is needed as the risk to the agency's information systems and data remains higher than acceptable. For example, the lack of monitoring capabilities for user account modifications, as well as the Commission not identifying and/or disabling inactive user accounts could increase the risk of unauthorized account creation and use. In particular, we found that account administrators had the ability to create new user accounts, modify data using that account, and then delete the account without detection. Additional improvements must be made by the Commission to comply with Federal laws and regulations related to protecting sensitive agency information. A lack of protection for this type of information increases the risk of potential compromise or use by unauthorized or malicious individuals.

The failure to correct identified weaknesses in a timely manner also increases the risk that known security weaknesses will not be corrected or mitigated. We found that the POA&Ms provided by the Commission lacked information critical for the agency to prioritize security deficiencies for mitigation. Our review of POA&M items for the three major systems and the General Support System revealed that 52 of the 73 open POA&M completion dates had been pushed back – some for as long as 23 months. Without additional improvements to the POA&M process, management's ability to adequately assess the performance of the program and ensure effective and timely closure of weaknesses could be hindered.

RECOMMENDATIONS

The weaknesses discovered during our evaluation were discussed with Commission officials. Notably, management stated that it had taken actions to identify the types of sensitive data used by the Commission and was working to implement protective measures. However, to help ensure an effective cyber security program, we recommend that the Commission's Chairman take the following actions:

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

2. Revise and update cyber security policies and procedures, as appropriate, to ensure consistency with Federal cyber security requirements, particularly in the area of protection of sensitive information; and,

3. Ensure that the POA&M process includes all required information to properly identify, track, and monitor actions to enhance the ability to complete corrective actions in a timely manner.

MANAGEMENT REACTION

Management concurred with each of the report's recommendations. Management added that it had initiated or completed actions designed to address weaknesses identified during our review. In particular, management disclosed that it was in the process of implementing enhanced monitoring of access controls. In addition, management commented that it had issued policy for protecting sensitive information and had taken additional steps to further enhance its POA&M process.

AUDITORS COMMENTS

Management's comments were responsive to our recommendations. Management's comments are included in their entirety in Appendix 3.

Appendix 1

OBJECTIVE

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

SCOPE

The audit was performed between June 2009 and September 2009 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 the audit objective, we:

- Reviewed Federal laws and regulations related to controls over information technology (IT) security such as the *Federal Information Security Management Act*, Office of Management and Budget Memoranda, and National Institute of Standards and Technology standards and guidance;

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

- Held discussions with officials from the Commission and reviewed relevant documentation;

- 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 by the OIG and the Government Accountability Office.

We conducted this evaluation in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the effort to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objective. Accordingly, 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 IT project management. 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 did not rely solely on computer-processed data to satisfy our objectives. However, in those instances where we did utilize computer-processed data, we confirmed the validity of the data, when appropriate, by reviewing supporting source documents.

An exit conference was held with Commission officials on October 27, 2009.

RELATED REPORTS

- *Evaluation Report of The Federal Energy Regulatory Commission's Unclassified Cyber Security Program- 2008* (DOE/IG- 0802, September 2008). The Federal Energy Regulatory Commission (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 were needed to reduce the risk of compromise to the Commission's business information systems and data to an acceptable level. 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 (IT) staff, insufficient attention had been given to ensuring that existing policies and procedures were implemented. We made several recommendations designed to assist in achieving this goal.

- *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 financial 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 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 Unclassified 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 IT resources and data to compromise.

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

Office of the
Executive Director

October 8, 2009

MEMORANDUM TO : Rickey R. Hass
Deputy Inspector General

FROM : Thomas R. Herlihy Thomas R Herlihy
Executive Director

SUBJECT : Management Comments on DOEIG Draft Evaluation Report titled "The Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2009"

We appreciate the opportunity to respond to the subject draft report. As you noted in the report, the Federal Energy Regulatory Commission (FERC) has taken a number of actions to improve its cyber security practices and to maintain a strong network defense against malicious intruders and other external threats. We acknowledge the IG findings and recommendations and thank the auditors for their assistance in helping the Commission improve its security posture.

Based on the results of this evaluation, and the Commission's subsequent actions to implement the IG recommendations, we believe the FERC has an effective security program that meets the requirements of FISMA. We are committed to safeguarding our IT infrastructure and to maintaining a robust cyber security program. Our specific responses to your audit are included below. If you require further assistance please contact Matt Sweet at (202) 502-8926.

RECOMMENDATION 1: Complete actions to address vulnerabilities identified in this report.

FERC concurs, and has taken the following corrective actions to address the access control vulnerabilities identified in this report:

1) **Develop and Implement account monitoring policy and procedures:** As discussed during the audit, the Commission recently updated its IT Audit Log Policy, and is implementing an automated log management framework to mitigate the Commission's identified audit log weaknesses. The Commission is currently completing the documentation and testing activities associated with this implementation the Audit Log Management task. The Commission acknowledges that the current Account Management Policy (*FERC IT Account Management Policy, February 23, 2009*) does not adequately define the requirement to record and audit user account modifications, however the Commission has addressed this requirement in the recently created IT Audit Log Policy (*FERC IT Audit Log Policy, February 18, 2009*) and forthcoming audit log procedures. Additionally, the Commission is updating its Account Management Policy to refine the requirement to record and audit user account modifications.

   The IT Audit Log Policy defines at a high level what information and what types of devices require logging while the forthcoming procedures are to provide details on how logging is performed (tools used), who performs the log monitoring, type of events to monitor, frequency, and retention procedures.

The Commission is in the process of updating the Account Management Policy, IT Audit Log Policy and supporting procedures to ensure that it explicitly defines the requirements for the capture and management review of account modification events. Both policies and supporting procedures will be updated by 12/31/2009. The Commission is progressing to fully remediate this vulnerability.

2) **Perform a Commission-wide periodic review of all user accounts and related access privileges:** The annual recertification of all accounts, that was incomplete at the time of the audit, was completed on 9/30/2009.

3) **Protection of Sensitive Information**: Addressed as part of implementing Recommendation 2.

4) **Plan of Action and Milestones**: Addressed as part of implementing Recommendation 3.

RECOMMENDATION 2 – Revise and update cyber security policies and procedures as appropriate, to ensure consistency with Federal cyber security requirements, particularly in the area of protection of sensitive information.

FERC concurs with the Protection of Sensitive Information recommendations provided and has taken the following corrective actions to implement them:

1) The Commission has issued a policy to define what types of information should be considered sensitive and how this information should be protected during transmission. The Security and Systems Assurance Division will work with system owners to ensure the development and implementation of the appropriate procedures to comply with these policies as required.

2) By policy the Commission does not allow transmission of sensitive data, however to overcome this limitation, the Commission is evaluating various technologies to ensure adequate protection of sensitive data during transmission.

RECOMMENDATION 3 – Ensure that the Plan of Action and Milestones (POA&M) process includes all required information to properly identify, track, and monitor actions to enhance the ability to complete corrective actions in a timely manner.

FERC concurs in principle with the POA&M recommendations provided by the IG and has taken the following corrective actions:

1) **Update POA&M Reporting Template:** The Commission developed and implemented a C&A Policy (*FERC Certification & Accreditation Policy*, March 10, 2009), C&A Handbook (*FERC IT Certification & Accreditation (C&A) Handbook*, April 20, 2009) and a customized POA&M Reporting Database Tool during FY2009 in order to mitigate last years' POA&M findings.

   The C&A policy directs Commission staff to document POA&Ms and manage the mitigation of vulnerabilities identified through the C&A process (section 3). The Handbook details the methodology and steps required to complete a C&A -including continuous monitoring (section 8) and management of POA&Ms (section 5.5).

The FERC POA&M database tool provides management with the ability to track and report on all POA&Ms and POA&M related information such as:

- NIST 800-53 control requirements, test results, test artifacts, test dates, and control severity level.
- POA&M Milestone – milestone and task details
- POA&M ownership: the person responsible for planning and implementing tasks associated with closing the milestone.
- Estimated target completion dates: the date submitted by the POA&M/milestone owner intended to identify when a task is expected to be completed.
- Current Due Date: the date submitted by POA&M/milestone owner intended to identify the "updated" due date with a documented accounting of delays and new target dates.
- POA&M closed dates – Date the milestone was closed.

The Commission recognizes the fact that while we currently capture and review "*severity*" levels in the POA&M database tool, we do not currently provide reporting of the "*severity*" data field on the POA&M reporting template. The Commission also recognizes the OMB requirement to add a "*budget*" field to our POA&M template. The POA&M report has been updated to include these required fields.

The Commission also understands that, even though we actively use widely-accepted project management reporting tools (e.g. Project Management Plans and an executive dashboard) to provide management with effective project oversight and up to date milestone activity details, we are still required to further document these milestones on the POA&M report. The Commission has already updated the reporting template to meet the IG's recommendation.

2) **Update and implement policies and procedures on POA&M management:**
As detailed above, the Commission recently developed and implemented its POA&M C&A policies and procedures in FY 2009 to include POA&M management. The Commission recognizes the need to update its documentation and implement the required changes as identified above. Utilizing periodic audits and enhanced communication with management, we will ensure the policies are implemented correctly.

IG Report No. DOE/IG-0830

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 Felicia Jones at (202) 253-2162.

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.