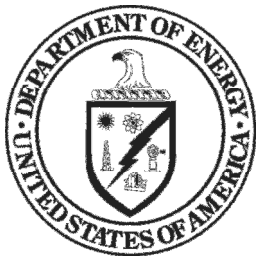

U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

Evaluation Report

The Federal Energy Regulatory Commission's Unclassified Cyber Security Program - 2011

OAS-M-12-01 November 2011

Department of Energy
Washington, DC 20585

November 15, 2011

MEMORANDUM FOR THE CHAIRMAN, FEDERAL ENERGY REGULATORY COMMISSION

FROM: Rickey R. Hass
Deputy Inspector General
for Audits and Inspections
Office of Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Federal Energy Regulatory Commission's Unclassified Cyber Security Program - 2011"

INTRODUCTION AND OBJECTIVE

The Federal Energy Regulatory Commission (Commission) is an independent agency within the Department of Energy responsible for regulating the Nation's oil pipeline, natural gas, hydroelectric and wholesale electric industries. The Commission relies on a wide range of information technology (IT) resources in achieving its mission of assisting consumers in obtaining reliable, efficient, and sustainable energy services. As highlighted by cyber attacks at various Federal entities over recent years, malicious individuals continue to take advantage of the changing information security threat landscape and exploit vulnerabilities in IT resources that have not been remediated. To help protect against cyber security threats such as these, the Commission estimated that it would expend approximately $3.8 million during Fiscal Year (FY) 2011 to secure its IT assets.

The Federal Information Security Management Act of 2002 (FISMA) established requirements for Federal agencies related to the management and oversight of information security risks and to ensure that IT resources were adequately protected. As directed by FISMA, the Office of Inspector General conducted an independent evaluation of the Commission's unclassified cyber security program to determine whether it adequately protected data and information systems. This report presents the results of our evaluation for FY 2011.

RESULTS OF EVALUATION

The Commission had taken actions to improve its cyber security posture and mitigate risks associated with certain issues identified during our FY 2010 evaluation. While these measures are noteworthy, our current evaluation disclosed that additional action is needed to further protect information systems and data. In particular, we continued to identify weaknesses related to the Commission's timely remediation of software vulnerabilities. Specifically, our testing found that additional opportunities existed for the Commission to ensure that all servers and workstations were patched in a timely manner.

The problems we identified were due, in part, to less than fully effective implementation of cyber security policies and procedures. In particular, Commission officials informed us that they did

not follow existing Vulnerability Management Program (VMP) policies due to budget and resource constraints. Although the Commission continued to make progress in improving its cyber security posture, additional actions are needed to further reduce the risk to the agency's information systems and data.

The Commission had taken actions to improve its cyber security posture and mitigate risks associated with certain issues identified during our FY 2010 evaluation. For example the Commission had updated its incident response process to help ensure that all incidents were reported to the Department of Energy Cyber Incident Response Capability within established timeframes. In addition, it utilized its VMP to help identify vulnerabilities in unclassified network systems, including servers, workstations, applications, and network and security devices. Finally, officials continued to perform regularly scheduled scans of networks, workstations and web applications. These actions are positive; however, additional effort is needed. As such, we recommended that the Commission ensure that existing vulnerability management procedures are fully implemented.

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

MANAGEMENT REACTION

Management concurred with the report's recommendation and disclosed that it had initiated actions to address the issues identified in our report. Management's comments are included in their entirety in Appendix 3.

Attachment

cc: Deputy Secretary
Associate Deputy Secretary
Executive Director, Federal Energy Regulatory Commission
Chief of Staff

EVALUATION REPORT ON THE FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBER SECURITY PROGRAM - 2011

TABLE OF CONTENTS

Program Improvements and Patch Management

We identified a number of positive aspects related to the Federal Energy Regulatory Commission's (Commission) unclassified cyber security program. For instance, we noted that corrective actions had been taken to address certain issues identified during the Fiscal Year (FY) 2010 evaluation. We found that the Commission:

- Updated its incident response process to help ensure that all incidents were reported to the Department of Energy Cyber Incident Response Capability within established timeframes;
- Utilized its Vulnerability Management Program (VMP) to help identify vulnerabilities for its unclassified network systems, including servers, workstations, applications, and network and security devices; and,
- Continued to perform regularly scheduled scans of networks, workstations and web applications.

Patch Management

We determined that the Commission significantly reduced the number of "high risk" vulnerabilities in its information systems since our prior year review. In preliminary comments on our draft report, management stated that it had successfully applied over 500 patches to its almost 1,500 servers and workstations during FY 2011; activity covering over 95 percent of total available patches. Additionally, officials stated that certain patches could not be applied because they could have had operational impacts.

While these are positive results, our testing found that additional opportunities existed for the Commission to ensure that all servers and workstations were patched in a timely manner. Specifically, we noted that 32 of 70 vulnerabilities we identified were rated "high risk" by the vendor and/or the National Vulnerability Database sponsored by the Department of Homeland Security's National Cyber Security Division. While 9 of the issues identified impacted a significant number of the 45 servers and/or 236 workstations tested, the remaining 23 were confined to small subset of those devices.

The vulnerabilities we observed were primarily associated with third-party productivity and internet applications. Affected

systems included servers and workstations utilized by financial application users and system administrators with privileged levels of access to financial systems and general support systems. All of the "high risk" vulnerabilities identified were more than 30 days old, including 18 that were missing patches more than 1 year old. Furthermore, we identified several instances where the Commission was using software that was no longer supported by the vendor. As noted by the National Institute of Standards and Technology, proactively identifying and remediating system vulnerabilities can reduce or eliminate the potential for exploitation and involves considerably less time than responding to an exploit.

Cyber Security Policy Implementation

The problems we identified were due, in part, to less than fully effective implementation of cyber security policies and procedures. In particular, Commission officials informed us that they did not follow their existing VMP policies due to budget and resource constraints. As such, the identified "high risk" vulnerabilities on network server and workstation systems had not been remediated in a timely manner. While there are many nuances that must be considered when managing the use of existing resources, it is important to ensure that "high risk" vulnerabilities such as those identified during our review receive adequate attention and are addressed in a timely manner.

In addition, although the Commission had identified and tracked the vulnerabilities found during our testing in its Vulnerability Tracking Tool, officials had not followed the remediation timeframes required by its VMP procedures. For example, the VMP required that "high risk" vulnerabilities be remediated within 30 days. However, our testing found that each of the identified "high risk" weaknesses had significantly exceeded the prescribed timeframe for remediation.

Risk to Commission Systems and Information

Although the Commission continued to make progress in improving its cyber security posture, additional actions are needed to further reduce the risk to the agency's information systems and data. In particular, network servers and workstations running applications that were missing security updates for known vulnerabilities or were no longer supported by the vendor were at a heightened risk for malicious attacks that could result in the compromise of vulnerable systems. For example, an attacker could exploit the vulnerabilities to gain unauthorized access to systems, applications and sensitive data, including financial systems and data, which could disrupt normal business operations or have negative impacts on system and data reliability.

Additionally, workstations were at risk for computer viruses and other malicious vulnerability exploits that could provide attackers with complete control of those systems, and other devices residing on the internal network.

RECOMMENDATION

To correct the weaknesses identified in this report and improve the effectiveness of the Commission's unclassified cyber security program, we recommend that the Executive Director, Federal Energy Regulatory Commission, take the following action:

- Fully implement existing vulnerability and patch management procedures to ensure that security vulnerabilities are remediated and verified in a timely manner.

MANAGEMENT REACTION

Management concurred with the report's recommendation and commented that it had initiated actions to address weaknesses identified during our evaluation. In particular, management commented that it was aware of the vulnerabilities identified during our review and would resolve them through existing remediation plans by the end of 2011. In addition, management stated that it would continue to actively monitor all vulnerabilities in addition to any new threats identified through the use of security tools and alerts communicated from external sources.

AUDITOR COMMENTS

Management's comments were responsive to our recommendation. 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 evaluation was performed between July 2011 and November 2011, at the Commission's Headquarters in Washington, DC. KPMG LLP (KPMG), assisted the Office of Inspector General (OIG) by performing an assessment of the Commission's unclassified cyber security program. Our evaluation also included a review of general and application controls in areas such as security management, access controls, configuration management, segregation of duties, and contingency planning.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Federal laws and regulations related to controls over information technology security such as the *Federal Information Security Management Act of 2002*, Office of Management and Budget Memoranda, and National Institute of Standards and Technology standards and guidance;

- Evaluated the Commission in conjunction with its annual audit of the Financial Statements, utilizing work performed by KPMG. OIG and KPMG work included analysis and testing of general and application controls for the network and systems and review of the network configuration;

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

- Held discussions with Commission officials and reviewed relevant documentation; and,

- Reviewed prior reports issued by the OIG and the U.S. 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 audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit 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 its information and unclassified cyber security program. 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 to satisfy our objective. In particular, computer assisted audit tools were used to perform probes of various networks and drives. We validated the results of the scans by confirming the weaknesses disclosed with responsible on-site personnel and performed other procedures to satisfy ourselves as to the reliability and competence of the data produced by the tests.

Management waived an exit conference.

RELATED REPORTS

- *The Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2010*, (OAS-M-11-01, October 2010). The Federal Energy Regulatory Commission (Commission) had taken actions to significantly improve its cyber security posture and mitigate risks associated with each of the four weaknesses we identified during our Fiscal Year (FY) 2009 evaluation. However, additional action was needed to improve protection of information systems and data. Specifically, we found that security patches needed to resolve known vulnerabilities discovered during regularly scheduled scans were not applied to all workstations in a timely manner. In addition, even though officials had established an automated mechanism for tracking all known vulnerabilities, only 10 percent of the identified "high risk" vulnerabilities were actually being tracked. The problems we identified with the Commission's unclassified cyber security program were due, in part, to the less than fully effective implementation of policies and procedures. As such, the risk to the agency's information systems and data remained higher than necessary. Management concurred with the report's recommendations and commented that it had initiated actions to address weaknesses identified during our evaluation.

- *The Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2009*, (DOE/IG-0830, October 2009). The Commission had taken steps to improve its unclassified cyber security program; however, additional actions were necessary to help ensure the networks, systems and data were adequately protected against increasingly sophisticated cyber security attacks. 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. The Commission's Plan of Action and Milestones process for addressing cyber security weaknesses did not include all information necessary to ensure effectiveness. Absent improvement, the risk to the agency's information systems and data remains higher than necessary. Management concurred with the report's recommendations and commented that it had initiated or already completed actions to address weaknesses identified during our evaluation.

- *The Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2008* (DOE/IG-0802, September 2008). While the Commission had taken action to improve its unclassified cyber security program, our evaluation disclosed that additional actions were needed to reduce the risk of compromise to 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 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. Management concurred with the report's recommendations and stated that measures were being taken to ensure that issues identified in our report were being addressed.

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

Office of the
Executive Director

November 01, 2011

MEMORANDUM TO: Rickey R. Hass
Deputy Inspector General for Audit Services

FROM Charles H. Schneider
Executive Director

SUBJECT Management Comments on DOEIG Draft Evaluation Report titled "The Federal Energy Regulatory Commission's Unclassified Cyber Security Program -2011"

We appreciate the opportunity to respond to the subject draft report. As noted by the Inspector General's (IG) office, in this year's Annual FISMA report, the Federal Energy Regulatory Commission (FERC) has taken many positive actions to improve its cyber security practices and to maintain a strong network defense against malicious intruders and other external threats. We understand the IG's finding during this year's audit and appreciate the recommendations and observations provided. We thank the auditors for their assistance to the Commission in improving our security posture.

Based on the actions taken as a result of this year's evaluation, and with significant consideration given to the IG recommendations, we believe the FERC will continue to maintain an effective security program that achieves 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 Sanjay Sardar, Deputy CIO, at (202) 502-6634, or Anton Porter, Deputy CFO, at (202) 502 -8728.

RECOMMENDATION 1 – Vulnerability Management: Fully implement existing vulnerability and patch management procedures to ensure that security vulnerabilities are remediated and verified in a timely manner.

The Federal Energy Regulatory Commission (FERC), through the use of our Vulnerability Management Program (VMP), has been aware of the identified vulnerabilities. The FERC's VMP has greatly matured in the past fiscal year showing effective processes in actively identifying and tracking vulnerabilities. While the FERC has successfully addressed many of the identified vulnerabilities, due to resource constraints, we were not able to fully remediate. Vulnerability management is taken very seriously, as such, we will strongly consider the IG's recommendation and strive to further improve. The FERC will continue to actively monitor all vulnerabilities in addition to any new threats identified through the use of security tools and alerts communicated from external approved resources. We will continue to push our existing remediation plans to resolve all identified issues before the end of CY 2011.

Public

IG Report No. OAS-M-12-01

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://energy.gov/ig

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