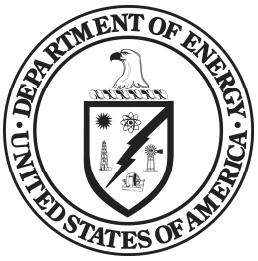

U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

Evaluation Report

The Federal Energy Regulatory Commission's Unclassified Cyber Security Program - 2012

OAS-L-13-01

November 2012

Department of Energy
Washington, DC 20585

November 7, 2012

MEMORANDUM FOR THE EXECUTIVE DIRECTOR, FEDERAL ENERGY REGULATORY COMMISSION

FROM: Daniel M. Weeber
Assistant Inspector General
for Audits and Administration
Office of Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Federal Energy Regulatory Commission's Unclassified Cyber Security Program - 2012"

BACKGROUND

The Federal Energy Regulatory Commission (Commission) is an independent agency within the Department of Energy responsible for, among other things, regulating interstate transmission of the Nation's electricity, natural gas and oil. In addition, the Commission licenses and inspects private, municipal and state hydroelectric projects. To achieve its mission, the Commission relies on a wide range of information technology (IT) resources to help ensure that rates and terms and conditions for the wholesale of electric energy and natural gas are just and reasonable, and promote the development of a safe, reliable and efficient energy infrastructure. As highlighted by recent cyber attacks on Federal entities, the information security threat landscape continues to change, and vulnerable IT resources continue to be exploited. To help protect against continuing cyber security threats, the Commission estimated that it would expend approximately $5.3 million during Fiscal Year (FY) 2012 to secure its IT assets, a 39 percent increase from FY 2011.

The Federal Information Security Management Act of 2002 (FISMA) established requirements for Federal agencies regarding 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 2012.

CONCLUSIONS AND OBSERVATIONS

The Commission had taken action to further improve its cyber security posture and mitigate risks associated with the weaknesses identified during our FY 2011 evaluation. While these actions are noteworthy, our current evaluation disclosed that additional opportunities existed to better protect its information systems and data. Specifically, we continued to identify weaknesses related to the Commission's timely remediation of software vulnerabilities.

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

Positive Aspects

We identified a number of positive measures taken by the Commission related to enhancing its unclassified cyber security program. For instance, we noted that the Commission continued to make improvements in implementing the existing Vulnerability Management Program (VMP). Specifically, we found that the Commission:

- Initiated a project to upgrade the software tool used to manage patch and software deployment. Officials stated that completion of this project is expected in late 2012 and should reduce the need to manually update systems; and,

- Had identified and continued to monitor vulnerabilities through its VMP and Plan of Action and Milestones (POA&M) processes.

Patch Management

Although significant progress had been made to secure the Commission's network devices, servers and workstations, our testing identified additional opportunities for it to ensure that all devices were patched in a timely manner. Specifically, of the 337 workstations tested, 33 contained vulnerable productivity applications, and 105 workstations were using software utilities that had not been patched. All of the vulnerabilities were considered to be high risk by the vendor and were more than 90 days old, including some affecting workstations that were more than 2 years old. Affected systems included workstations utilized by financial application users and system administrators with privileged levels of access to financial systems and general support systems. 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. Notably, our scans of network devices and servers did not identify any significant vulnerabilities.

Policy Implementation

As in past years, the problems we identified with the Commission's vulnerability management process were due, in part, to less than fully effective implementation of policies and procedures. In particular, although action had been taken to strengthen the Commission's VMP and POA&M processes, our review of weaknesses in the POA&M disclosed that 35 high- and medium-risk vulnerabilities had not been remediated based on the VMP-defined remediation timeframes. 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 vulnerabilities had significantly exceeded the prescribed timeframe for remediation.

In addition, 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 had not been remediated in a timely manner. Officials stated, and we agree, that successful completion of the Commission's ongoing project to update its patch management tools should further enhance its VMP.

Risks to 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, workstations running vulnerable applications and utilities were at a heightened risk for malicious attacks that could result in the compromise of those systems and/or the information contained within them. 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.

SUGGESTED ACTION

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

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

We appreciate the cooperation of the Commission and its ongoing efforts to ensure that its unclassified cyber security program is managed efficiently and effectively. Because no recommendations are being made in this report, a formal response is not required.

Attachment

cc: Deputy Secretary
Associate Deputy Secretary
Chief of Staff

OBJECTIVE, SCOPE AND METHODOLOGY

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 May 2012 and November 2012, at the Commission's Headquarters in Washington, DC. Specifically, KPMG, LLP (KPMG), the Office of Inspector General's (OIG) contract auditor, 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.

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 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 *GPRA Modernization Act of 2010* and determined that it had not established performance measures for its 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.

PRIOR REPORTS

- Evaluation Report on *The Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2011*, (OAS-M-12-01, November 2011). The Federal Energy Regulatory Commission (Commission) had taken actions to improve its cyber security posture and mitigate risks associated with certain issues identified during our Fiscal Year (FY) 2010 evaluation. While these measures were noteworthy, our evaluation disclosed that additional action was needed to further protect information systems and data. Specifically, we continued to identify weaknesses related to the Commission's timely remediation of software vulnerabilities. The problems we identified with the Commission's vulnerability management program were due, in part, to less than fully effective implementation of policies and procedures. Although the Commission continued to make progress in improving its cyber security posture, additional actions were needed to further reduce the risk to the agency's information systems and data. Management concurred with the report's recommendations and commented that it had initiated actions to address weaknesses identified during our evaluation.

- Evaluation Report on *The Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2010*, (OAS-M-11-01, October 2010). The 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 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.

- Evaluation Report on *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. Management concurred with the report's recommendations and commented that it had initiated or already completed actions to address weaknesses identified during our evaluation.

IG Report No. OAS-L-13-01

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 applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit or 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 that 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 our office 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.