



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 – 2013

OAS-M-14-01

October 2013



Department of Energy
Washington, DC 20585

October 23, 2013

MEMORANDUM FOR THE EXECUTIVE DIRECTOR, FEDERAL ENERGY
REGULATORY COMMISSION

A handwritten signature in black ink, appearing to read "Rickey R. Hass".

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 – 2013"

BACKGROUND

The Federal Energy Regulatory Commission (Commission) is an independent agency within the Department of Energy (Department) responsible for, among other things, regulating the interstate transmission of the Nation's electricity, natural gas and oil. To realize its mission, the Commission gathers and analyzes significant amounts of data related to energy markets, using a wide range of information technology resources. As highlighted by recent cyber attacks on Federal entities, including the Department, the information security threat of a breach or loss of information technology assets or information contained in these assets continues to increase as attacks become more sophisticated and prevalent. To help protect against continuing cyber security threats, the Commission estimated that it would spend approximately \$5.8 million during Fiscal Year (FY) 2013 to secure its information technology assets, a 9 percent increase compared to FY 2012.

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 information technology 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 2013.

RESULTS OF EVALUATION

The Commission had taken action to improve its cyber security posture and mitigate risks associated with the weaknesses identified during our FY 2012 evaluation. Our current evaluation, however, disclosed that additional opportunities existed to better protect information systems and data. In particular, 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 with detailed information regarding identified vulnerabilities and, in certain instances, had initiated corrective action.

Positive Aspects

The Commission had taken a number of positive actions related to enhancing its unclassified cyber security program. For example, the Commission continued to make improvements in implementing the existing Vulnerability Management Program. Specifically, we found that the Commission:

- Continued implementation of a project to upgrade the software tool used to manage patch and software deployment. This project is expected to be completed in October 2013 and should reduce the need to manually update systems.
- Effectively designed and operated general and application information technology controls such as access controls and contingency planning measures to protect its information.
- Created a process to implement longstanding missing patches. Specifically, Commission officials conducted weekly status meetings to discuss and prioritize outstanding software patches so that critical and high-risk patches are tested and implemented. Officials told us that they hoped to have longstanding missing patch issues resolved by November 2013.

Patch Management

Although progress had been made to secure the Commission's servers and workstations, our review of Commission vulnerability scan results identified additional opportunities for it to ensure that all devices were patched in a timely manner. Specifically, we noted:

- 132 workstations and servers contained vulnerable productivity applications;
- 114 workstations and servers were using vulnerable software utilities;
- 23 workstations and servers had antivirus applications with known vulnerabilities; and
- 460 workstations and servers had utilized vulnerable web browser applications.

Each of the vulnerabilities were considered to be critical or high risk; however, we were unable to determine how long the vulnerabilities existed in the environment based on the information provided by Commission officials. 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 exploitation of vulnerabilities.

Policy Implementation

Similar to prior years, the problems we identified with the Commission's Vulnerability Management Program were due, in part, to policies and procedures that were not fully effective. Specifically, even though the Commission had taken action to strengthen its Vulnerability Management Program, our review found that the Commission had not fully updated existing security patch management and vulnerability management processes and technical controls to address the recommended actions. We determined that vulnerabilities similar in type, frequency and risk level to those identified during our FY 2012 evaluation continue to exist in the Commission's information technology environment. Officials stated, and we agree, that successful completion of the Commission's ongoing project to update its Vulnerability Management Program policies and patch management technologies is important to maintaining an effective security posture.

Risks to Commission Systems and Information

The Commission had continued to make progress in improving its cyber security posture; however, additional actions are needed to reduce the risk to the agency's information systems and data. For instance, workstations and network servers 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 those systems. We noted that 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.

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:

- Update, as needed, and implement existing vulnerability and patch management procedures to ensure that security vulnerabilities are remediated and verified in a timely manner, in accordance with the Vulnerability Management Program.

MANAGEMENT REACTION

The Commission concurred with the report's recommended action and stated that it had initiated corrective action to address weaknesses identified in the report. In particular, management commented that the Commission is in the process of reviewing and updating all existing policies, procedures and security program documentation related to vulnerability and patch management.

AUDITOR COMMENTS

Management's comments were responsive to our recommendation and are included in Attachment 3.

Attachments

cc: 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 and October 2013, at the Commission's Headquarters in Washington, DC. Specifically, KPMG, LLP (KPMG), the Office of Inspector General's 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. In addition, KPMG reviewed the Commission's results of workstation and server authenticated scans for the period of May and June 2013.

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. Office of Inspector General 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.
- Reviewed prior reports issued by the Office of Inspector General 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 evaluation objective. Accordingly, we assessed significant internal controls and the Commission's implementation of the *GPRA Modernization Act of 2010* and determined that it had established a performance measure 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, KPMG reviewed the results of authenticated scans for workstations and servers for the period of May and June 2013. We validated the results of the scans by confirming the weaknesses disclosed with responsible on-site personnel.

An exit conference was waived by the Commission.

PRIOR REPORTS

- Evaluation Report on [*The Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2012*](#), (OAS-L-13-01, November 2012). The Federal Energy Regulatory Commission (Commission) had taken actions to improve its cyber security posture and mitigate risks associated with weaknesses identified during our Fiscal Year (FY) 2011 evaluation. While these actions are noteworthy, our evaluation disclosed 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. 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 addition, Commission officials informed us that they did not follow their existing Vulnerability Management Program policies due to budget and resource constraints. As corrective action was initiated by management in certain instances, we made a suggestion to update existing vulnerability and patch management procedures as needed to ensure that security vulnerabilities are remediated and verified in a timely manner.
- Evaluation Report on [*The Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2011*](#), (OAS-M-12-01, November 2011). 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 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.

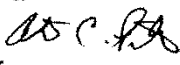
MANAGEMENT COMMENTS

**FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, DC 20426**

**Office of the
Executive Director**

October 17, 2013

MEMORANDUM TO: Rickey R. Hass
Deputy Inspector General for Audits & Inspections
Department of Energy

FROM: Anton C. Porter 
Executive Director

CC: Sanjay Sardar
Chief Information Officer

W. Doug Foster
Chief Financial Officer

Naeem Musa
Chief Information Security Officer

Elizabeth Hensley
Audit Liaison

SUBJECT: Management Comments on DOEIG Draft Evaluation Report titled "The Federal Energy Regulatory Commission's Unclassified Cyber Security Program -2013"

We appreciate the opportunity to respond to the subject draft report. As noted by the 2013 Department of Energy (DOE) Inspector General's (IG) office Annual FISMA report, the Federal Energy Regulatory Commission (Commission) 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 made. 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 Commission 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 Naeem Musa, CISO, at (202) 502-8468, or Elizabeth Hensley, Audit Liaison, at (202) 502 -6240.

RECOMMENDATION 1 – Vulnerability Management: Update and implement existing procedures related to vulnerability and patch management to ensure timely remediation of security vulnerabilities.

The Commission continues to take positive actions to ensure a strong security posture that supports the confidentiality, integrity and availability of its mission critical systems and data. Though the Commission continues to identify, track and remediate vulnerabilities within our environment, we concur in principle with the Vulnerability Management recommendation provided. The Commission understands vulnerability management is an ongoing effort that requires continuous attention with the support of reliable and effective technologies. The Commission has already taken steps to implement mitigations as detailed below:

1. The Commission is in the process of reviewing and updating all existing policies, procedures, and security program documentation surrounding vulnerability and patch management. In addition, all federal and contractor staff involved in the vulnerability remediation process are being trained more frequently to ensure complete understanding of their roles and responsibilities.
2. The Commission is in the process of upgrading the Microsoft System Center Configuration Manager and deploying Microsoft Windows 7 to all user workstations to more effectively track, deploy, and monitor security patches and vulnerabilities impacting the infrastructure.
3. The Commission has applied to become an early adopter of the Department of Homeland Security (DHS) Continuous Diagnostic Monitoring Program. This program will allow the Commission to procure, through external appropriations, additional and more effective technologies to increase the security posture.
4. The Commission's IT Security staff continues working closely with the United States Computer Emergency Readiness Team, DHS National Cyber and Communications Integration Center, and the DOE Joint Cybersecurity Coordination Center to stay informed of all newly discovered critical vulnerabilities. The Commission continues to utilize this information to react in a timely fashion and mitigate against all newly reported critical exploits in near real time.

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 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 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.