



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 – 2010

OAS-M-11-01

October 2010



Department of Energy
Washington, DC 20585

October 25, 2010

MEMORANDUM FOR THE CHAIRMAN, FEDERAL ENERGY REGULATORY
COMMISSION

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

FROM: Rickey R. Hass
Deputy Inspector General for Audit Services
Office of Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Federal
Energy Regulatory Commission's Unclassified Cyber Security
Program – 2010"

BACKGROUND

The Federal Energy Regulatory Commission (Commission) is responsible for regulating and overseeing the interstate transmission of natural gas, oil and electricity in addition to numerous other natural gas and hydroelectric projects. The regulations set forth by the Commission are designed to meet the economic, environmental and safety interests of the Nation. The Commission gathers and analyzes massive amounts of data regarding the energy markets, using a wide range of information technology (IT) resources. As with other Federal agencies or private institutions, the threat of a breach or loss of IT assets or information they contain continues to increase as cyber attacks become more sophisticated and prevalent. To protect against such threats, the Commission expected to spend over \$3.5 million during Fiscal Year (FY) 2010 to secure its IT assets.

The Federal Information Security Management Act of 2002 (FISMA) provides direction to agencies on the management and oversight of information security risks. Under FISMA's requirements, the Office of Inspector General conducts an annual independent evaluation to determine if the Commission's unclassified cyber security program is properly aligned with FISMA. This report presents the results of our evaluation for FY 2010.

RESULTS OF EVALUATION

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. Testing during our current evaluation, however, revealed that additional action is 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 ten 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. Specifically, contrary to established Commission policies, officials failed to formally accept the risks associated with not addressing known software vulnerabilities. As such, the risk to the agency's information systems and data remained higher than necessary.

Since the completion of the FY 2009 evaluation, the Commission had made significant progress in the enhancement of its unclassified cyber security program. For example, officials had taken action to address each of the weaknesses we identified in the prior year related to account modification and monitoring, network account management, and protection of sensitive information. In addition, the Commission enhanced its plan of action and milestones database to include more specificity to help manage the cyber security program. These actions are positive; however, additional effort is needed to help strengthen the protection of the Commission's information systems and data. As such, we have made a recommendation that, if fully implemented, should help the Commission further improve its cyber security posture.

Our evaluation also revealed an issue related to maintenance of the Commission's IT inventory that is more fully discussed in Appendix 1.

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 recommendation and disclosed that it had initiated actions to address issues identified in our report. Management's comments are included in their entirety in Appendix 4.

Attachment

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

**EVALUATION REPORT ON THE FEDERAL ENERGY
REGULATORY COMMISSION'S UNCLASSIFIED CYBER
SECURITY PROGRAM – 2010**

**TABLE OF
CONTENTS**

Commission's Unclassified Cyber Security Program

Details of Finding1
Recommendation and Comments3

Appendices

1. Other Matters for Consideration.....4
2. Objective, Scope, and Methodology5
3. Related Reports7
4. Management Comments8

The Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2010

Program Improvements

The Federal Energy Regulatory Commission (Commission) continued to make progress in enhancing its unclassified cyber security program and addressing previously identified cyber security issues. Specifically, we noted that corrective actions had been taken to address each of the four weaknesses identified during the Fiscal Year (FY) 2009 review. In particular, the Commission:

- Had taken action to remediate previously identified access control weaknesses in the areas of account modification monitoring and network account management;
- Enhanced its policies and procedures related to protection of sensitive information and ensured that sensitive information was encrypted when in transit; and,
- Made improvements to its plan of action and milestones database containing weaknesses identified during security control testing, to include increased specificity to help manage the cyber security program.

Risk Management and Security Controls

Despite improvements in the management of its unclassified cyber security program, additional action is needed to further reduce the risk of compromise to the Commission's information systems and data. In particular, we identified weaknesses in the area of vulnerability management.

Vulnerability Management

While the Commission had identified various vulnerabilities during the performance of regularly scheduled scans of networks, workstations and web applications, officials had not ensured that all workstations were patched in a timely manner. Specifically, our performance testing identified 7 commercial off-the-shelf (COTS) software products utilized by the Commission that contained more than 600 vulnerabilities on 28 workstations. Of the vulnerabilities identified, we noted that 445 (73 percent) were rated "high risk" by the National Vulnerability Database sponsored by the Department of Homeland Security's National Cyber Security Division/US-CERT. In addition, 59 of the "high risk" vulnerabilities were more than 2 years old. The vulnerabilities were primarily associated with third-party productivity and internet

applications. Officials noted that they had initiated installation of version upgrades to certain software products that could eliminate many of the identified vulnerabilities. In addition, our testing did not reveal any actual exploits of the vulnerabilities identified.

Furthermore, even though the Commission had established the Vulnerability Tracking Tool (VTT) to track scanning-related weaknesses identified as part of its continuous monitoring program, all known vulnerabilities were not included in the application. Specifically, only 43 of 445 (10 percent) "high risk" vulnerabilities identified during our performance testing were tracked in the VTT. In addition, a number of the vulnerabilities identified were input into the VTT only after we brought them to management's attention. We did note that one item included in the VTT related to a specific application that included various individual vulnerabilities. While we could not confirm how many vulnerabilities this item covered, it is likely that the percentage of weaknesses being tracked is actually higher. The table below summarizes the number of vulnerabilities identified and tracked in the VTT.

<u>Application</u>	<u>Total Vulnerabilities</u>	<u>High Risk Vulnerabilities</u>	<u>Tracked in VTT</u>
COTS - 1	110	93	13
COTS - 2	100	86	12
COTS - 3	58	47	8
COTS - 4	53	46	10
COTS - 5	159	93	0
COTS - 6	37	25	0
COTS - 7	92	55	0
<i>Total</i>	<i>609</i>	<i>445</i>	<i>43</i>

Tracking all known vulnerabilities in the VTT could help ensure that they receive the appropriate level of management attention.

Cyber Security Policy Implementation

The problems we identified with the Commission's unclassified cyber security program were due, in part, to a less than fully effective implementation of policies and procedures. In particular, contrary to established Commission policies related to vulnerability tracking and risk acceptance, we identified that officials had not formally accepted the risks associated with not addressing known software vulnerabilities. Specifically, cyber security officials stated that they had accepted the risks associated with vulnerabilities identified during our review

and, therefore, did not need to track the weaknesses. However, they were unable to provide documentation to support this assertion. Officials also noted that not all workstations could be patched because the software was no longer supported by the manufacturer. Per the Commission's Vulnerability Management Program Standard Operating Procedure, completion of a waiver was required in situations where these risks were being accepted. In addition, as noted by the National Institute of Standards and Technology, establishing an appropriate mechanism for tracking known security weaknesses can aid in ensuring that they are effectively remediated in a timely manner. In preliminary comments on our audit findings, officials noted that they were aware of the need to better document accepted risks and agreed to take necessary corrective actions.

**Risk to Commission
Systems and
Information**

While the Commission made progress in improving its cyber security posture over the past year, the risk to the agency's information systems and data remained higher than necessary. Specifically, failure to correct identified "high risk" weaknesses in a timely manner could increase the risk of exploitation of known security weaknesses, thereby compromising the Commission's systems. Without improvements in the implementation of vulnerability management policies and procedures, management's ability to adequately track all known security weaknesses could hinder timely remediation efforts.

RECOMMENDATION

To correct the weaknesses identified in this report and improve the effectiveness of the Commission's cyber security program, we recommend that the Executive Director, Federal Energy Regulatory Commission, take action to ensure that procedures related to vulnerability management are fully implemented in a timely manner, to include documenting the acceptance of risk, as appropriate.

**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 the Commission was in the process of reviewing and revising its VTT and remediating the vulnerabilities identified during our review.

AUDITOR COMMENTS

Management's comments were responsive to our recommendation. Management's comments are included in their entirety in Appendix 4.

OTHER MATTERS FOR CONSIDERATION

In addition to the weaknesses discussed in this report related to the Federal Energy Regulatory Commission's (Commission) unclassified cyber security program, we identified a separate area for consideration. Specifically, we noted that the Commission's information technology (IT) hardware inventory was not accurate or complete. For instance, we found that 11 items sampled had been excessed, but still remained on the inventory listing in the Sunflower system. In some instances, these items remained in the system for up to two years after being sent to the General Services Administration for reuse. We also identified an instance where the Commission had not included all servers within the Sunflower system. Rather, officials only tracked the casing that contained the servers. Furthermore, we identified one instance where a laptop had been incorrectly categorized as general hardware within Sunflower.

These issues occurred because the Commission had not adhered to its established procedures for inventory management. Specifically, the Commission's Property Management Standard Operating Procedures required that the asset management system be updated within one business day of property being transferred. However, as noted above, we identified inventory that still remained in the system even though it had been removed from the site approximately 2 years prior to our review. In addition, while Commission representatives stated that an annual inventory of all hardware had been conducted as a compensating control to offset the lack of a complete IT listing, these controls did not ensure that officials would be able to effectively identify whether inventory had been lost or stolen.

SUGGESTION FOR IMPROVEMENT

To correct the weaknesses identified, we suggest that the Executive Director, Federal Energy Regulatory Commission, take action, as appropriate to ensure that the Commission's Property Management procedures are fully implemented, to include timely reporting of inventory actions.

Appendix 2

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 2010 and September 2010, at the Commission's Headquarters in Washington, DC. 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 certification and accreditation, security configuration management, incident response and reporting, and plans of action and milestones. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Federal laws and regulations related to controls over information technology (IT) 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;
- Reviewed the Commission's overall cyber security program, including 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 prior reports issued by the OIG and the Government Accountability Office.

We conducted this audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit 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 findings and conclusions based on our audit objectives. 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 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 did not solely rely on computer-processed data to satisfy our objective. However, 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. In addition, we confirmed the validity of other data, when appropriate, by reviewing supporting source documents.

An exit conference was waived by Commission officials.

RELATED REPORTS

Office of Inspector General Reports

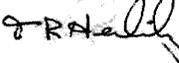
- *The Federal Energy Regulatory Commission's Unclassified Cyber Security Program - 2009* (DOE/IG-0830, October 2009). The Federal Energy Regulatory Commission (Commission) had taken steps to improve its cyber security program based on the deficiencies identified during the Fiscal Year 2008 review. However, additional actions were necessary to help ensure the Commission's network, systems and data are 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, the audit team discovered that officials had not always effectively implemented existing policy and/or corrected previously observed weaknesses. It was also noted that 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.
- *The Federal Energy Regulatory Commission's Unclassified Cyber Security Program - 2008* (DOE/IG-0802, September 2008). The Commission had taken action to improve cyber security practices and implemented protective measures designed to defend its networks against malicious attackers and other external threats. Our evaluation, however, disclosed that additional actions are needed to reduce the risk of compromise to the Commission's business information systems and data to an acceptable level. 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.
- *The Federal Energy Regulatory Commission's Cyber Security Program - 2007* (OAS-L-07-23, September 2007). Overall, we continued to note improvements in the Commission's cyber security program. During our evaluation, we found that a major financial processing system had undergone a significant software upgrade in 2005, but the system had not been recertified and reaccredited for operation. Because of the nature of the software upgrade, significant changes occurred both in the manner in which data was processed and how it was transmitted – a situation that could have potentially introduced security vulnerabilities or increased the risk associated with system upgrade. Commission officials provided evidence that they 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.

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

Office of the
Executive Director

October 13, 2010

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

FROM: Thomas R. Herlihy 
Executive Director

SUBJECT: Management Comments on DOEIG Draft Evaluation Report titled "The Federal Energy Regulatory Commission's Unclassified Cyber Security Program -2010"

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 findings 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: Ensure procedures related to vulnerability management are fully implemented in a timely manner, to include documenting the acceptance of risk as appropriate.

Though the FERC has always tracked vulnerabilities to our environment with vigilance, we concur in principal with the Vulnerability Management recommendation provided. While the vulnerabilities identified in this year's audit had been previously identified by the FERC and the risk to the environment had been accepted, we recognize the documentation of this acceptance was not complete. The FERC understands that we must be more disciplined in documenting the risks that apply and we have already taken steps to implement mitigations as detailed below:

1. The Commission is in the process of reviewing and revising its Vulnerability Tracking Tool (VTT) to ensure all vulnerabilities will be actively tracked and monitored on a periodic basis. In addition to continuing to perform monthly vulnerability scans and post all results on our centralized IT Security Program site, we will utilize these scan results as a compensating measure to ensure all vulnerabilities discovered are tracked, remediated or accepted as timely as possible.
2. The FERC is currently in the process of remediating the seven (7) COTS product vulnerabilities identified during the fieldwork performed by the Inspector General. The majority of the COTS product vulnerabilities identified represents one (1) software package that has multiple components. Although FERC was already aware of these vulnerabilities, action was not taken in part due to compatibility issues between the new software release and the current operating system. Since the time the vulnerability assessment testing was performed by the IG, the FERC has already mitigated 95% of all identified vulnerabilities and on target to mitigate 100% of the remaining vulnerabilities.

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.