U.S. Department of Energy

Office of Inspector General

Office of Audits and Inspections

EVALUATION REPORT

The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2014

OAS-L-15-03

October 2014

Department of Energy
Washington, DC 20585

November 3, 2014

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 Cybersecurity Program – 2014"

BACKGROUND

The Federal Energy Regulatory Commission (Commission) is an independent agency within the Department of Energy responsible for, among other things, regulating the interstate transmission of the Nation's electricity, natural gas and oil. To accomplish its mission, the Commission utilizes significant amounts of energy market data using a wide range of information technology resources. As attacks become more sophisticated and prevalent, the threat of a breach or loss of information technology assets or information contained in these assets continues to increase.

The *Federal Information Security Management Act of 2002* (FISMA) established requirements for Federal agencies to develop, implement and manage agency-wide information security programs, including management and oversight of information security risks to ensure that information technology resources are adequately protected. As directed by FISMA, the Office of Inspector General conducted an independent evaluation of the Commission's unclassified cybersecurity program to determine whether it adequately protected data and information systems. This report presents the results of our evaluation for Fiscal Year (FY) 2014.

RESULTS OF EVALUATION

During our current year evaluation, we found that the Commission had taken positive action to improve its cybersecurity program and mitigate risks associated with past weaknesses. In particular, the Commission made improvements to its security patch management and vulnerability management program to address weaknesses identified during our prior evaluations.

Cybersecurity Management

Our review disclosed that the Commission had updated existing security patch management and vulnerability management procedures to address the prior recommended actions related to timely remediation of software vulnerabilities. We also found that the Commission's general

information technology controls were adequately designed and operating effectively to provide reasonable assurance of the integrity, confidentiality and availability of data in financial applications. We determined that the risk and frequency of identified vulnerabilities was significantly reduced from the prior year's test results. While we identified certain vulnerabilities on servers and workstations supporting critical nonfinancial applications and data, we found that risk mitigation and/or compensating controls were in place that may help the Commission identify or prevent attacks targeting its systems. Further, the Commission documented the acceptance of risk associated with several of the identified weaknesses and had initiated remediation actions to address the vulnerabilities. Based on the results of our FY 2014 testwork, we determined that the prior year's notice of finding and recommendation related to vulnerability management had been remediated.

Attachment

cc: Deputy Secretary
Chief of Staff

OBJECTIVE, SCOPE AND METHODOLOGY

OBJECTIVE

To determine whether the Federal Energy Regulatory Commission's (Commission) unclassified cybersecurity program adequately protected data and information systems.

SCOPE

The evaluation was performed between June and October 2014 at the Commission's Headquarters in Washington, DC. Specifically, KPMG, LLP, the Office of Inspector General's contract auditor, performed an assessment of the Commission's unclassified cybersecurity 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, LLP performed a vulnerability assessment on the networks and systems managed by the Commission.

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, LLP. Office of Inspector General and KPMG, LLP 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 cybersecurity 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 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 evaluation 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 cybersecurity 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.

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions and feedback to OIGReports@hq.doe.gov and include your name, contact information and the report number. Comments may also be mailed to:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 253-2162.