U.S. Department of Energy

Office of Inspector General

Office of Audits and Inspections

AUDIT REPORT

Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2015

OAI-L-16-02

October 2015

Department of Energy
Washington, DC 20585

October 30, 2015

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: Audit Report: "Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2015"

BACKGROUND

The Federal Energy Regulatory Commission (Commission), an independent agency within the Department of Energy, was established to regulate major aspects of the Nation's wholesale electric, natural gas, hydroelectric, and oil pipeline industries. The Commission's information technology infrastructure must be dependable and resilient to support its missions. To that end, officials noted that they received approximately $2.5 million in fiscal year 2015 to secure the Commission's unclassified systems and information.

The *Federal Information Security Modernization Act of 2014* (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. In addition, Federal agencies must provide acceptable levels of security for the information and systems that support their operations and assets. Further, FISMA mandated that agency Offices of Inspector General conduct annual independent evaluations to determine whether agencies' unclassified cybersecurity programs adequately protected data and information systems. This report presents the results of our evaluation for the Commission for fiscal year 2015.

RESULTS OF AUDIT

Our fiscal year 2015 audit work found that the Commission had implemented the tested attributes of its cybersecurity program in a manner that was generally consistent with requirements established by the National Institute of Standards and Technology, the Office of Management and Budget, and the Department of Homeland Security. In particular, as a result of testing on a sample of targets within the Commission's unclassified internal network, including servers and workstations, nothing came to our attention to indicate that management, operating, and technical controls implemented within that environment were not operating effectively.

Based on our testwork, we concluded that the Commission's unclassified cybersecurity program had implemented the main attributes required by the Department of Homeland Security in each of the major topic areas tested. These topic areas included configuration management, identity and access management, incident response and reporting, risk management, security training, plans of action and milestones, remote access management, contingency planning, and contractor-managed systems. In addition, we determined that the Commission had defined and initiated implementation of a continuous monitoring program based on the maturity model developed by the Council of the Inspectors General for Integrity and Efficiency. However, the Commission had not fully implemented its continuous monitoring program.

Because nothing came to our attention that would indicate significant control weaknesses in the areas tested, we are not making any recommendations or suggested actions relative to this audit.

Attachment

cc: Deputy Secretary
Chief of Staff

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

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

SCOPE

The audit was performed between June and October 2015 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 cybersecurity program. This 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 performed a vulnerability assessment on selected portions of the networks and systems managed by the Commission and reviewed the Commission's implementation of the *Federal Information Security Modernization Act of 2014* (FISMA). The audit was conducted under Office of Inspector General project number A15TG042.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Federal laws and regulations related to cybersecurity, such as FISMA, 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 selected portions of the Commission's network and systems, technical review of the network configuration, and assessment of compliance with the requirements of FISMA, as established by the Office of Management and Budget and the Department of Homeland Security.

- 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 audit 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 established a performance measure for its information and unclassified cybersecurity program. Because our audit was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. 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 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 OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to us:

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.