OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

EVALUATION REPORT

OAI-L-17-01

November 2016

FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2016

Department of Energy
Washington, DC 20585

November 4, 2016

MEMORANDUM FOR THE EXECUTIVE DIRECTOR, FEDERAL ENERGY REGULATORY COMMISSION

FROM: Sarah B. Nelson
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 – 2016"

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. The Commission's mission is to assist consumers in obtaining reliable, efficient, and sustainable energy services at a reasonable cost through appropriate regulatory and market means. To accomplish this, the information technology that supports the Commission must be reliable and protected against attacks from malicious sources.

The *Federal Information Security Modernization Act of 2014* established requirements for Federal agencies to develop, implement, and manage agency-wide information security programs, including periodic assessment of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. In addition, the *Federal Information Security Modernization Act of 2014* mandated that an independent evaluation be performed annually by the Office of Inspector General to determine the effectiveness of the agency's information security program and practices. The Office of Inspector General contracted with KPMG LLP (KPMG) to perform an assessment of the Commission's unclassified cybersecurity program. This report presents the results of that evaluation for fiscal year 2016.

RESULTS OF AUDIT

Fiscal year 2016 audit work, performed by KPMG, 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, testing on a

sample of targets within the Commission's unclassified internal network, including servers and workstations, found that management, operating, and technical controls implemented within that environment were effective.

Based on testwork performed by KPMG, we concluded that attributes required by the Office of Management and Budget and the Department of Homeland Security were implemented into the Commission's unclassified cybersecurity program for each of the major topic areas tested. These topic areas included risk management, contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring, incident response, and contingency planning. In addition, we concluded, based on the results of KPMG's testwork, 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 on Integrity and Efficiency. Although the Commission had strengthened its continuous monitoring program compared to the previous year, it was not yet fully implemented.

Because nothing came to our attention that would indicate significant control weaknesses in the areas tested by KPMG, 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's (Commission) unclassified cybersecurity program adequately protected data and information systems.

SCOPE

The evaluation was performed between June 2016 and November 2016 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).

METHODOLOGY

To accomplish our objective, we:

- Reviewed Federal laws and regulations related to Federal 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. This 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.

Management waived an exit conference on October 27, 2016.

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.