OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

EVALUATION REPORT

DOE-OIG-18-06

October 2017

FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBERSECURITY PROGRAM - 2017

Department of Energy
Washington, DC 20585

October 27, 2017

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 – 2017"

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 and transportation 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 infrastructure 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 systems and data 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 whether the Commission's unclassified cybersecurity program adequately protected data and information systems. The Office of Inspector General contracted with KPMG LLP to perform an assessment of the Commission's unclassified cybersecurity program. This report presents the results of that evaluation for fiscal year 2017.

RESULTS OF EVALUATION

Based on fiscal year 2017 test work performed by KPMG LLP, nothing came to our attention to indicate that attributes required by the Office of Management and Budget, Department of Homeland Security, and the National Institute of Standards and Technology were not

incorporated into the Commission's unclassified cybersecurity program for each of the major topic areas tested. In particular, the Commission had implemented information technology security controls for various areas such as configuration management, risk management, and security training. For instance, testing on multiple targets within the Commission's unclassified internal network, including servers and workstations, found the technical controls implemented within that environment were effective.

However, near the completion of our test work, we became aware of a recent security incident involving the Commission's unclassified cybersecurity program. Upon learning of the incident, Commission officials initiated action to identify the cause of the incident, determine its impact, and implement corrective actions, as necessary. While we commend the Commission for its response to the security incident, we are concerned that certain controls may not have been in place that could have potentially prevented the incident. At the time of our test work, the Commission was still in the process of determining the impact of the incident.

RECOMMENDATION

To help improve the Commission's unclassified cybersecurity program, we recommend that the Executive Director for the Commission:

1. Ensure that the analyses related to the cyber incident identified in our report are completed in a timely manner and that any remaining corrective actions related to implementation of preventative controls are appropriately prioritized.

MANAGEMENT REACTION

Management concurred with the recommended action and indicated that corrective actions had been taken or were initiated to address the issues identified in the report. Management's formal comments are included in Attachment 2.

AUDITOR COMMENTS

Management's comments and corrective actions were responsive to our recommendation. We appreciate the cooperation received from your staff during our review.

Attachments

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 2017 and October 2017 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. This included a review of general and application controls related to security management, access controls, configuration management, segregation of duties, and contingency planning. In addition, KPMG LLP performed a vulnerability assessment on selected portions of the networks, servers, and workstations managed by the Commission and reviewed the Commission's implementation of the *Federal Information Security Modernization Act of 2014*. This evaluation was conducted under Office of Inspector General project number A17TG036.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Federal laws and regulations related to cybersecurity, such as *Federal Information Security Modernization Act of 2014*, 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. 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 the *Federal Information Security Modernization Act of 2014*, 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 officials waived an exit conference on October 26, 2017.

MANAGEMENT COMMENTS

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, DC 20426

Office of the
Executive Director

October 24, 2017

MEMORANDUM TO: Sarah B. Nelson
Assistant Inspector General
for Audits and Administration

FROM: Anton Porter
Executive Director

SUBJECT: Management Comments on DOEIG Evaluation Report on the "Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2017"

We appreciate the opportunity to respond to the subject report. As you noted in the report, the Federal Energy Regulatory Commission (FERC) has implemented information technology security controls for various areas such as configuration management, risk management, and security training. We strive to improve our cybersecurity practices on a continuous basis to maintain a strong network defense against malicious intruders and other external threats. Based on the results of this evaluation and the Commission's proactive actions to implement the IG recommendations, we believe the FERC has an effective security program that meets the requirements of federal mandates. Our specific responses to your recommendation are included below:

RECOMMENDATION 1: "Ensure that the analyses related to the cyber incident identified in our report are completed in a timely manner and that any remaining corrective actions related to the implementation of preventative controls are appropriately prioritized."

FERC OED Management Response: Upon discovery of the incident, the Commission immediately contained, mitigated, and performed comprehensive after action activities to appropriately respond to the incident referenced by the IG. FERC also in parallel, initiated its analysis to determine the scope and impact to Commission resources. FERC is currently working with DOE to continue the analysis of the impact of the security incident. FERC is collaborating with DOE and will finalize its analysis in a timely manner.

As part of FERC's proactive approach to comprehensive risk management, the Commission continually assesses security controls, provides weighted impact scores and manages risk mitigation activities utilizing the enterprise's Plan of Action and Milestones (POA&M). The vector utilized in this incident had previously been identified and POA&M mitigation milestones were in the process of being completed when the incident occurred. To date, the Commission has enacted security controls to provide reasonable assurance of preventing similar incidents and continues to close out all milestones associated with the specific POA&M.

The Office of the Executive Director has made significant investments to enhance the Commission's incident response capabilities and this is evident as the Commission scored a "Level 4" maturity based

on the Inspector General annual FISMA metrics. These advanced capabilities has allowed FERC to respond quickly and appropriately to cyber event investigations and potential incidents.

These efforts represent FERC's proactive commitment to continually strengthening FERC's unclassified cybersecurity program. We are happy to provide additional information regarding this incident, our containment efforts, and our continuing work to keep FERC's systems and data secure. We acknowledge the Inspector General's recommendations and thank the auditors for their assistance in helping the Commission improve its security posture.

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.