OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

EVALUATION REPORT

DOE-OIG-19-09

December 2018

FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBERSECURITY PROGRAM - 2018

Department of Energy
Washington, DC 20585

December 14, 2018

MEMORANDUM FOR THE EXECUTIVE DIRECTOR, FEDERAL ENERGY REGULATORY COMMISSION

FROM: Sarah B. Nelson
Assistant Inspector General
for Technology, Financial, and Analytics
Office of Inspector General

SUBJECT: INFORMATION: Evaluation Report on the "Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2018"

BACKGROUND

The Federal Energy Regulatory Commission (FERC) 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. FERC'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 FERC 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 FERC's unclassified cybersecurity program adequately protected data and information systems. The Office of Inspector General contracted with KPMG LLP to perform an assessment of FERC's unclassified cybersecurity program. This report presents the results of that evaluation for fiscal year 2018.

RESULTS OF EVALUATION

Based on fiscal year 2018 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 FERC's unclassified cybersecurity program for each of the major topic areas tested. In particular, FERC had implemented information technology security controls for various areas such as configuration management, risk management, and security training.

During our fiscal year 2017 test work, we became aware of a security incident involving FERC's unclassified cybersecurity program. Upon learning of the incident, FERC officials initiated action to identify the cause of the incident, determine its impact, and implement corrective actions, as necessary. While FERC's corrective actions taken related to the implementation of preventative controls are noteworthy, we found that FERC was still in the process of reviewing the impact of the incident and completing its analysis.

RECOMMENDATION

Consistent with the recommendation included in our prior year's evaluation, until all corrective actions are completed, we continue to recommend that the Executive Director, Federal Energy Regulatory Commission:

1. Ensure that the analysis related to the cyber incident identified in our report is completed in a timely manner.

MANAGEMENT RESPONSE

Management provided corrective actions that were responsive to our recommendation. Management stated that FERC initiated its analysis immediately to determine the scope and impact of the cyber incident. Management also indicated that the analysis was completed in November 2018, and a full incident report will be provided to the Office of Inspector General in December 2018. Management's formal comments are included in Attachment 2.

AUDITOR COMMENTS

Management's comments and corrective actions were responsive to our recommendation. While management indicated that the analysis related to the cyber incident would be provided to us in December 2018, the analysis had not been provided to us prior to the conclusion of our review.

Attachments

cc: Deputy Secretary
Chief of Staff
Chief Information Officer

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective of this evaluation was to determine whether the Federal Energy Regulatory Commission's (FERC's) unclassified cybersecurity program adequately protected data and information systems.

SCOPE

The evaluation was performed between June 2018 and December 2018 at FERC's Headquarters in Washington, DC. Specifically, KPMG LLP, the Office of Inspector General's contractor auditor, performed an assessment of FERC'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 reviewed FERC's implementation of the *Federal Information Security Modernization Act of 2014*. This evaluation was conducted under Office of Inspector General project number A18TG035.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Federal laws and regulations related to cybersecurity, such as the *Federal Information Security Modernization Act of 2014*, Office of Management and Budget memoranda, and National Institute of Standards and Technology standards and guidance;

- Evaluated FERC 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 FERC's network and systems, and an 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 FERC officials and reviewed relevant documentation; and

- Reviewed prior reports issued by the Office of Inspector General and the Government Accountability Office.

Management officials waived an exit conference on December 10, 2018.

MANAGEMENT COMMENTS

FEDERAL ENERGY REGULATORY COMMISSION

Washington, DC 20426

December 3, 2018

Office of the Executive Director

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

FROM: Anton Porter
Executive Director

SUBJECT: Management Comments on DOEIG Evaluation Report on the "Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2018"

We appreciate the opportunity to respond to the subject report. As you noted, 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: "Ensure that the analysis related to the cyber incident identified in our report is completed in a timely manner."

FERC OED Management Response: Upon discovery, the Commission immediately contained, mitigated, and performed comprehensive after action activities to appropriately respond to the incident referenced by the IG. FERC, in parallel, also initiated its analysis to determine the scope and impact to Commission resources. Due to the size and complexity of the incident, FERC management assigned multiple subject matter experts from each of the affected program offices to provide detailed analysis of the lost data. That analysis was completed in November 2018 and a full incident report will be provided to the IG in December 2018.

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 FISMA metrics. These advanced capabilities have 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 recommendation 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) 586-7406.