OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

EVALUATION REPORT

DOE-OIG-20-07

November 2019

FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBERSECURITY PROGRAM - 2019

Department of Energy
Washington, DC 20585

November 13, 2019

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 – 2019"

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 a periodic assessment of the risk and magnitude of 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 (KPMG) to perform an assessment of FERC's unclassified cybersecurity program. This report presents the results of that evaluation for fiscal year 2019.

RESULTS OF EVALUATION

Based on fiscal year 2019 test work performed by KPMG, we determined that FERC had implemented the tested attributes of its cybersecurity program in a manner that was generally

consistent with Federal requirements. In particular, we found no indications that management, operating, and technical controls implemented within FERC's information technology environment were not effective.

Test work performed by KPMG concluded that cybersecurity attributes required by the Office of Management and Budget, Department of Homeland Security, and the National Institute of Standards and Technology were generally incorporated into FERC's unclassified cybersecurity program for each of the major topic areas tested. Using the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* issued by the Council of the Inspectors General on Integrity and Efficiency, KPMG evaluated FERC's security posture in eight topic areas. Based on test work conducted by KPMG, we determined that FERC had achieved a calculated maturity level of "optimized" in the areas of risk management, configuration management, identity and access management, data protection and privacy, security training, and information security continuous monitoring. In addition, FERC had "managed and measurable" performance related to incident response and had "consistently implemented" a contingency planning program.

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 evaluation.

Attachment

cc: Deputy Secretary
Chief of Staff
Chief Information Officer
Chief Financial Officer, Federal Energy Regulatory Commission
Chief Information Officer, Federal Energy Regulatory Commission

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

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

SCOPE

The evaluation was performed between June 2019 and October 2019 at FERC 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 A19TG036.

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 memorandum, 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, as well as 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.

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

Management waived an exit conference on October 10, 2019.

PRIOR REPORTS

- Evaluation Report on *Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2018* (DOE-OIG-19-09, December 2018). Based on fiscal year 2018 test work performed by KPMG LLP, we concluded that the Federal Energy Regulatory Commission had implemented information technology security controls for various areas such as configuration management, risk management, and security training. However, we made one recommendation related to ensuring that the Federal Energy Regulatory Commission completed its analysis regarding a cybersecurity incident in a timely manner.

- Evaluation Report on *Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2017* (DOE-OIG-18-06, October 2017). Based on test work performed, nothing came to our attention to indicate that attributes required by the Department of Homeland Security, Office of Management and Budget, and the National Institute of Standards and Technology were not incorporated into the Federal Energy Regulatory Commission's unclassified cybersecurity program for the topics tested. We made one recommendation related to ensuring that the Federal Energy Regulatory Commission completed an analysis regarding a cybersecurity incident in a timely manner.

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) 586-1818. For media-related inquiries, please call (202) 586-7406.