Office of Inspector General

OFFICE OF TECHNOLOGY, FINANCIAL, AND ANALYTICS

EVALUATION REPORT -

THE FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2020

DOE-OIG-21-16
FEBRUARY 2021

Department of Energy
Washington, DC 20585

February 22, 2021

Memorandum for the Executive Director

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

Subject: Evaluation Report on "The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2020"

What We Reviewed and Why

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, document, and implement 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 agency's operations and assets. In addition, the *Federal Information Security Modernization Act of 2014* mandated that the Office of Inspector General annually perform an independent evaluation of the agency's unclassified cybersecurity program. The Office of Inspector General contracted with KPMG LLP to perform an assessment of FERC's unclassified cybersecurity program. The objective of the evaluation was to determine whether FERC's unclassified cybersecurity program adequately protected data and information systems. This report presents the results of that evaluation for fiscal year 2020.

What We Found

Based on fiscal year 2020 test work performed by KPMG LLP, we found that attributes required by the Office of Management and Budget and the National Institute of Standards and Technology were incorporated into FERC's unclassified cybersecurity program for each of the major topic areas tested. For instance, we determined that FERC had implemented information technology security controls for various areas such as risk management, data protection and privacy, and security training, among others.

While FERC's cybersecurity program was effective overall, we identified a segregation of duties issue in a FERC application. Specifically, we found that a user was granted conflicting privileges in the system that created an internal control weakness. Although FERC had designed a control to prevent such an issue from occurring, it had not been effectively implemented. This issue was concerning because the conflicting roles could have potentially allowed the user to both create and approve certain items in the system. Given the segregation of duties weakness, we issued a notice of finding and recommendations to FERC.

In addition, using the *FY 2020 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 LLP evaluated FERC's security posture in eight topic areas. Based on the results of the test work, 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 achieved "managed and measurable" performance related to incident response and had "consistently implemented" a contingency planning program.

Subsequent to our test work, it was reported that Federal agencies, including the Department and FERC, encountered a serious and sophisticated cyberattack. Due to the timing of our review, we did not evaluate the circumstances surrounding any potential impacts to FERC or how such an attack could have impacted our results, if at all. We will continue to follow developments related to any potential impacts as we continue our future test work.

What We Recommend

To address the segregation of duties issue, we recommended that FERC:

1. Implement a segregation of duties monitoring control to identify conflicting or inappropriate roles in the financial application; and

2. Perform the implemented monitoring control on a more frequent basis.

Management Comments

Management concurred with the recommendations and indicated that corrective actions had been taken to address the issue identified in the report. Management's formal comments are included in Appendix 3.

Office of Inspector General Response

Management's comments and corrective actions are responsive to the recommendations, and we will validate the corrective actions during our fiscal year 2021 evaluation.

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

Appendix 1

Objective, Scope, and Methodology

Objective

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

Scope

The evaluation was performed from June 2020 through February 2021 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 A20TG016.

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.

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

An exit conference was waived by FERC management on February 2, 2021.

Appendix 2

Prior Reports

- Evaluation Report on the Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2019 (DOE-OIG-20-07). Based on fiscal year 2019 test work performed by KPMG LLP, we determined that the Federal Energy Regulatory Commission (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 LLP 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.

- Evaluation Report on the Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2018 (DOE-OIG-19-09). Based on fiscal year 2018 test work performed by KPMG LLP, we found that cybersecurity attributes required by the Office of Management and Budget, Department of Homeland Security, and the National Institute of Standards and Technology were 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. However, 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.

Management Comments

FEDERAL ENERGY REGULATORY COMMISSION

Washington, DC 20426

January 22, 2021

Office of the Executive Director

MEMORANDUM TO: Sarah B. Nelson
Assistant inspector General
for Technology, Financial, and Analytics
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 – 2020"

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 risk management, data protection and privacy, and security training, among others. We strive to improve our cybersecurity practices on a continuous basis to maintain a strong network defense against malicious intruders and other 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: "Implement a segregation of duties monitoring control to identify conflicting or inappropriate roles in the financial application; and Perform the implemented monitoring control on a more frequent basis."

FERC OED Management Response: During the evaluation, it was uncovered that a recently promoted employee within the Financial Management Division was granted conflicting privileges. Collectively the two conflicting roles contain the system privileges for the employee to enter and post a general ledger journal, which infringes upon established separation of duties. Though FERC had a control in place to prevent this from occurring, it did not properly work. While preventing a single employee from having conflicting system roles is a control designed to uphold the integrity of FERC's financial statements, it is not the only control. More specifically, the allocation of system roles is only one component of an overarching risk management framework that consists of: the active promotion of internal polices; continuous training; recurring employee background investigations; spontaneous peer reviews; and downstream financial reconciliations/safeguards. The significance of these other compensating controls is not trivial, which FERC corroborated through the presentation and full disclosure of FERC's financial system's general ledger system audit logs. Specifically, FERC compiled and presented every general ledger entry that the employee came in contact with during fiscal year 2020. The review unconditionally proved that not a single violation of the targeted 'separation of duty' had occurred.

Nevertheless, FERC fully recognizes the importance of strengthening the execution and enforcement of our existing internal controls and committed to implementing the following corrective actions:

- Implement a process that adds transparency into the current and final state of an end-user's financial system access. Specifically, along with the conventional System Access Request form, FITT will generate a report that itemizes all of the end-user's existing permissions within the financial application and email it to the Accounting Officer for review. If the Accounting Officer approves the new system privileges, then FITT will execute the updates within the application and regenerate another report that captures the end state of the end-user's total access within the system and submit it to the Accounting Officer for confirmation. Collectively the 'before' and 'after' security profile snapshots will enable the approver the ability to identify any separation of duties violations in real-time.

- Perform an independent security access review on a monthly basis.

Corrective actions were implemented October 2020. The Accounting Officer now and since receives a before/after individual report, and also performs a monthly review of all profile changes and digitally signs off on those reviews.

These efforts represent FERC's proactive commitment to continually strengthening FERC's unclassified cybersecurity program. We are happy to provide additional information regarding this issue, our corrective actions implemented, 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.

cc: Chief Financial Officer, Federal Energy Regulatory Commission
Chief Information Officer, Federal Energy Regulatory Commission
Chief Information Security Officer, Federal Energy Regulatory Commission

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.