Office of Inspector General

OFFICE OF CYBER ASSESSMENTS AND DATA ANALYTICS

SUMMARY REPORT

THE FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2022

DOE-OIG-23-11
NOVEMBER 2022

Department of Energy
Washington, DC 20585

November 28, 2022

Memorandum for the Executive Director

From: Kshemendra Paul
Assistant Inspector General
for Cyber Assessments and Data Analytics
Office of Inspector General

Subject: Summary Report on The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2022

What We Reviewed and Why

The Federal Energy Regulatory Commission (FERC) is an independent agency within the Department of Energy that assists consumers in obtaining economically efficient, safe, reliable, and secure energy services at a reasonable cost through appropriate regulatory and market means, and collaborative efforts. FERC's statutory authority centers on major aspects of the Nation's wholesale electric, natural gas, hydroelectric, and oil pipeline industries. Congress has charged FERC with the development and review of, as well as compliance with, mandatory reliability standards for the bulk-power system to increase the system's reliability. In addition, FERC helps to secure the energy infrastructure from cyber and physical attacks through voluntary architecture assessments and the promotion of best practices to mitigate existing and emerging vulnerabilities. Given its mission and responsibilities, FERC's information technology environment must be reliable and protected against attacks from malicious sources.

The Federal Information Security Modernization Act of 2014 (FISMA) establishes requirements for Federal agencies to develop, implement, and manage agency-wide information security programs to ensure that information technology resources are adequately protected. FISMA also mandates that Inspectors General perform, on an annual basis, an independent evaluation of the agency's information security program. Our evaluation assessed FERC's cybersecurity program according to FISMA security metrics issued by the Department of Homeland Security, the Office of Management and Budget (OMB), and the Council of the Inspectors General on Integrity and Efficiency. As noted in the following table, these metrics are focused around five cybersecurity

functions and nine security domains that align with the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*.

Cybersecurity Functions		Security Domains
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Risk Management
		Supply Chain Risk Management
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services.	Configuration Management
		Identify and Access Management
		Data Protection and Privacy
		Security Training
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	Information Security Continuous Monitoring
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.	Incident Response
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	Contingency Planning

Source: *Framework for Improving Critical Infrastructure Cybersecurity* and FISMA security metrics issued by the Department of Homeland Security, OMB, and the Council of the Inspectors General on Integrity and Efficiency.

During fiscal year (FY) 2022, OMB altered its approach regarding how Inspectors General were to evaluate their agency's implementation of policies and procedures described by the National Institute of Standards and Technology. In particular, OMB and the Council of the Inspectors General on Integrity and Efficiency developed a multi-year cycle in which OMB selects a core group of metrics representing a combination of Administration priorities and other highly valuable controls that must be evaluated annually. The remaining metrics will be evaluated on a 2-year cycle. The core metrics for FY 2022 were chosen based on alignment with Executive Order 14028, *Improving the Nation's Cybersecurity*, as well as recent OMB guidance to agencies in furtherance of the modernization of Federal cybersecurity. According to OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, only the core metrics were required to be evaluated during FY 2022.

In response to the FISMA mandate, the Office of Inspector General contracted with KPMG LLP to assist in the assessment of FERC's unclassified cybersecurity program. We initiated this evaluation to determine whether FERC's unclassified cybersecurity program was implemented in accordance with Federal and Department requirements. This report summarizes the results of that evaluation for FY 2022.

What We Found

Our FY 2022 test work found that FERC 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, OMB, and the Department of Homeland

Security. In particular, we found no indications that management, operating, and technical controls implemented within FERC's information technology environment were ineffective.

Using the *FY 22 Core IG Metrics Implementation Analysis and Guidelines*, KPMG LLP evaluated FERC's security posture associated with the core metrics found within the nine security domains. Based on the results of the test work, we determined that FERC had achieved a calculated maturity level of "managed and measurable"[1] for its overall unclassified cybersecurity program. FERC's information security continuous monitoring activities had achieved a maturity level of "optimized" while its risk management, identify and access management, data protection and privacy, security training, incident response, and contingency planning achieved a maturity level of "managed and measurable." In addition, FERC had "consistently implemented" performance related to supply chain risk management and configuration management.

What We Recommend

Because nothing came to our attention that would indicate significant control weaknesses in the areas tested, we are not making any recommendations or suggested actions related to this evaluation.

Attachments

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

[1] According to the *FY 22 Core IG Metrics Implementation Analysis and Guidelines*, a Level 4, Managed and Measurable, information security program is considered operating at an effective level of security.

Objective, Scope, and Methodology

Objective

We initiated this evaluation to determine whether the Federal Energy Regulatory Commission's (FERC) unclassified cybersecurity program was implemented in accordance with Federal and Department of Energy requirements.

Scope

The evaluation was performed from April 2022 through November 2022 at FERC's Headquarters in Washington, DC. Specifically, KPMG LLP, the Office of Inspector General's contract auditor, assisted in the assessment of FERC's unclassified cybersecurity program. This included a review of information security policies and procedures that align with the five function areas in the *Framework for Improving Critical Infrastructure Cybersecurity*: Identify, Protect, Detect, Respond, and Recover. 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 A22TG012.

Methodology

To accomplish our objective, we:

- Reviewed Federal laws and regulations related to cybersecurity (e.g., 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 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 cybersecurity documentation.

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

An exit conference was waived by FERC management on November 2, 2022.

Related Reports

Office of Inspector General

- Evaluation Report on *The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2021* (DOE-OIG-22-07, November 2021). Based on fiscal year 2021 test work performed by KPMG LLP, we found that attributes required by the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology were incorporated into the Federal Energy Regulatory Commission's (FERC) unclassified cybersecurity program for each of the major topic areas tested. While FERC's cybersecurity program was effective overall, we found certain opportunities for improvement existed related to plan of action and milestones.

- Evaluation Report on *The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2020* (DOE-OIG-21-16, February 2021). Based on fiscal year 2020 test work performed by KPMG LLP, we found that attributes required by the Office of Management and Budget, the 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. While FERC's cybersecurity program was effective overall, we identified a segregation of duties issue in a FERC application. Given this weakness, we issued a notice of finding and recommendations to FERC management.

Government Accountability Office

- *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges* (GAO-21-288, March 2021).

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.