Office of Inspector General

OFFICE OF CYBER ASSESSMENTS AND DATA ANALYTICS

SUMMARY REPORT

THE FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2023

DOE-OIG-24-06
November 2023

Department of Energy
Washington, DC 20585

November 20, 2023

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 – 2023

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 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 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. FERC also helps to secure the energy infrastructure from cyber and physical attacks by encouraging utilities to invest in advanced cybersecurity technology and participate in cybersecurity threat information sharing. 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) established 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 developed 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 Table 1, the 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*.

Table 1.

Cybersecurity Functions		Security Categories
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, 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 actions 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 developed by the Department of Homeland Security, the OMB, and the Council of Inspectors General on Integrity and Efficiency.

Each year, OMB provides reporting guidance and deadlines to Executive Departments and agencies through a memorandum. The fiscal year (FY) 2023 guidance placed additional emphasis on implementing the requirements of Executive Order 14028, *Improving the Nation's Cybersecurity*,[1] and subsequent Administration actions to help ensure that agencies continue to drive forward with implementation of the requirements. As a result, the FY 2023 metric guidance was updated to determine agency progress in implementing requirements set forth within the OMB memorandum and Department of Homeland Security Binding Operational Directives in areas such as, but not limited to, asset management and discovery, vulnerability enumeration, supply chain security, incident detection and analysis, and strengthening of endpoint detection and response solutions and capabilities. In addition, the FISMA evaluation guidelines expanded on last year's core metric evaluation and added supplemental metrics that are assessed at least once every 2 years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

[1] Executive Order 14028 put forward a call to action to modernize and transform Federal systems to meet or exceed leading cybersecurity practices and focused on setting and establishing clear security requirements (applying multifactor authentication, encrypting data at rest and in transit, and improving endpoint detection and response); enhancing the integrity and transparency of the software supply chain; and creating the Cyber Safety Review Board to evaluate and learn from cyber incidents.

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 2023.

What We Found

Our FY 2023 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. We found no indications that management, operating, and technical controls implemented within FERC's information technology environment were ineffective.

Using the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, we 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 "optimized" for its overall unclassified cybersecurity program. FERC's identity and access management, data protection and privacy, security training, information security continuous monitoring, and contingency planning functions had achieved a maturity level of "optimized." FERC's risk management, supply chain risk management, configuration management, and incident response categories achieved a maturity level of "managed and measurable."[2]

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

[2] According to the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, achieving a Level 4, Managed and Measurable, or above 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 March 2023 through November 2023 at FERC's Headquarters in Washington, DC. 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 A23TG008.

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 3, 2023.

Related Reports

Office of Inspector General

- Evaluation Report on *The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2022* (DOE-OIG-23-11, November 2022). Based on the fiscal year 2022 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 Federal Energy Regulatory Commission's (FERC) unclassified cybersecurity program for each of the major topic areas tested. Nothing came to our attention that would indicate significant control weaknesses in the areas tested which resulted in no recommendations or suggested actions being made.

- 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 FERC's 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.

Government Accountability Office

- *CYBERSECURITY HIGH-RISK SERIES: Challenges in Protecting Cyber Critical Infrastructure* (GAO-23-106441, February 2023).

- *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.