Office of Inspector General

OFFICE OF CYBER ASSESSMENTS AND DATA ANALYTICS

SUMMARY REPORT

THE FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2024

DOE-OIG-25-08
DECEMBER 2024

Department of Energy
Washington, DC 20585

December 10, 2024

Memorandum for the Executive Director

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

Subject: Summary Report: *The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2024*

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 major responsibilities center on regulating the Nation's transmission and wholesale of electricity, transmission and sale of natural gas, and the transportation of oil by pipelines. FERC reviews proposals to build liquefied natural gas terminals and interstate natural gas pipelines, as well as licensing hydropower projects.

Pursuant to the Energy Policy Act of 2005, Congress tasked FERC to protect the reliability and cybersecurity of the bulk-power system through the establishment and enforcement of mandatory reliability standards, as well as additional authority to enforce FERC regulatory requirements. To accomplish this, FERC collaborates with regulated entities and other Federal and state governmental agencies to identify solutions to cyber and physical threats to FERC-jurisdictional infrastructure. Architecture assessments, physical security reviews, exercises, reviews of cybersecurity programs, and other activities are performed that assist in facilitating proactive efforts that prevent or mitigate loss or damage. Considering the agency's responsibilities, it is critical for FERC to manage a robust cybersecurity program to ensure threats are effectively mitigated and information remains secure.

The Federal Information Security Modernization Act of 2014 (FISMA) establishes requirements for Federal agencies to develop, document, and implement an agency-wide information security program to ensure that information technology resources are adequately protected. FISMA also

mandates that each agency annually performs an independent evaluation of the agency's information security program by its appointed Inspector General or by an independent external auditor as determined by the Inspector General. Our evaluation assessed FERC's unclassified cybersecurity program according to FISMA security metrics[1] developed by 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		Domain Areas
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
		Identity 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: The National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity* and *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.*

Each year, OMB provides reporting guidance and deadlines to Executive Departments and agencies through a memorandum. The fiscal year (FY) 2024 guidance places additional emphasis on implementing the requirements of Executive Order 14028, *Improving the Nation's Cybersecurity*,[2] and subsequent Administration actions to help ensure that agencies continue to drive forward with implementation of the requirements. As a result, the FY 2024 metric

[1] The FISMA metrics are broken into core and supplemental metrics. The core metrics are assessed annually and represent a combination of administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness. Conversely, the FISMA supplemental metrics 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.

[2] Executive Order 14028 puts forward a call to action to modernize and transform Federal systems to meet or exceed leading cybersecurity practices and focuses 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.

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 detection and remediation, supply chain security, incident response and reporting capabilities, and enhancing web and infrastructure security features.

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 adequately protected data and information systems in accordance with FISMA. This report summarizes the results of that evaluation for FY 2024.

What We Found

Our FY 2024 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. Based on our limited testing, we found no indications that the reviewed general information technology controls and business process application controls implemented within FERC's information technology environment were ineffective. Notably, our test work was limited only to a review of required FISMA metrics and select controls over financial processes. Our review did not include technical vulnerability testing.

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 and supplemental metrics found within the five function areas. We determined that FERC had achieved a calculated maturity level of "optimized" for its overall unclassified cybersecurity program. In particular, FERC had achieved a maturity level of "optimized" within the Protect, Detect, Respond, and Recover function areas while the Identify function area achieved a maturity level of "managed and measurable."[3]

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 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

[3] 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.

Attachment 1

Objective, Scope, and Methodology

Objective

We initiated this evaluation to determine whether the Federal Energy Regulatory Commission's (FERC) unclassified cybersecurity program adequately protected data and information systems in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).

Scope

While FERC Headquarters is in Washington, DC, the evaluation was performed remotely from March 2024 through December 2024. 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 National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*: Identify, Protect, Detect, Respond, and Recover. In addition, KPMG LLP reviewed FERC's implementation of FISMA. This evaluation was conducted under Office of Inspector General project number A24TG007.

Methodology

To accomplish our objective, we:

- Reviewed Federal laws and regulations related to cybersecurity (e.g., FISMA, 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, using work performed by KPMG LLP. This work included analysis and testing of general and application controls for selected portions of FERC's information systems and an assessment of compliance with the requirements of FISMA, 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 December 3, 2024.

Related Reports

Office of Inspector General

- Summary Report: *The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2023* (DOE-OIG-24-06, November 2023). Based on the fiscal year 2023 test work, we found that requirements established by the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology were implemented into the Federal Energy Regulatory Commission's unclassified cybersecurity program for each of the tested attributes. 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.

- Summary Report: *The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2022* (DOE-OIG-23-11, November 2022). Based on the fiscal year 2022 test work, we found that requirements established by the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology were implemented into the Federal Energy Regulatory Commission's unclassified cybersecurity program for each of the tested attributes. 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.

Government Accountability Office

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

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.