Office of Inspector General

OFFICE OF TECHNOLOGY, FINANCIAL, AND ANALYTICS

EVALUATION REPORT -

THE FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2021

DOE-OIG-22-07
NOVEMBER 2021

Department of Energy
Washington, DC 20585

November 15, 2021

Memorandum for the Executive Director

Sarah B. Nelson

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 – 2021

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, among other things, regulates the wholesale and interstate transmission of the Nation's electricity and natural gas and the pipeline transportation of oil. Further, FERC establishes standards to protect the reliability and cybersecurity of the bulk-power system. 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, 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 fiscal year (FY) 2021 FISMA security metrics.

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. The objective of the evaluation was to determine whether FERC's unclassified cybersecurity program adequately protected its data and information systems. This report presents the results of that evaluation for FY 2021.

What We Found

Our FY 2021 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, the Office of Management and Budget, and the Department of Homeland Security. In particular, we found that FERC had taken sufficient actions over the past year to address weaknesses related to separation of duties that were previously identified during our FY 2020 evaluation. As a result, we closed the prior year's finding. Our current review found no indications that management, operating, and technical controls implemented within FERC's information technology environment were ineffective.

While FERC's unclassified cybersecurity program was effective overall, we found that certain opportunities for improvement existed related to plans of action and milestones. In particular, although FERC had improved its process since our FY 2020 review, it did not always track required fields in accordance with its internal policy. Our review identified plans of action and milestones that excluded required information (e.g., the resources required, scheduled completion date, and milestone dates). As a result of this noted observation, followup testing of the plan of action and milestones process will be performed during next year's evaluation.

In addition, using the *FY 2021 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 nine topic areas. Based on the results of the test work, we determined that FERC had achieved a calculated maturity level of "managed and measurable" in the areas of risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning. In accordance with the Council of the Inspectors General on Integrity and Efficiency guidance, we did not incorporate metric ratings for the supply chain management domain into our consideration of the effectiveness of FERC's unclassified cybersecurity program because these ratings reference criteria that agencies were not required to implement at the time of our testing.

What We Recommend

Because nothing came to our attention that would indicate significant control weaknesses in the areas tested by KPMG LLP, we are not making any recommendations or suggested actions relative 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

Attachment 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 its data and information systems.

Scope

The evaluation was performed remotely from June 2021 through October 2021 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 A21TG017.

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 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 October 25, 2021.

Attachment 2

Related Reports

Office of Inspector General

- 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 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 identified a segregation of duties issue in a FERC application. Given this weakness, we issued a notice of finding and recommendations to FERC management.

- Evaluation Report on the *Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2019* (DOE-OIG-20-07, November 2019). Based on fiscal year 2019 test work performed by KPMG LLP, 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 ineffective. Test work performed by KPMG LLP concluded that cybersecurity attributes required by the Office of Management and Budget, the 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.

Government Accountability Office

- *HIGH-RISK SERIES: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges* (GAO-21-288, March 2021). The Government Accountability Office noted that Federal agencies and the Nation's infrastructure – such as energy, transportation systems, communications, and financial services – are dependent on information technology systems. The security of these systems and the data they use are vital to public confidence and national security, prosperity, and well-being. Given its impact, the Government Accountability Office has identified the four major cybersecurity challenges to include: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight; (2) securing Federal systems and information; (3) protecting cyber critical infrastructure; and (4) protecting privacy and sensitive data.

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.