U.S. DEPARTMENT OF ENERGY

Office of Inspector General

DOE-OIG-26-12

February 6, 2026

The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program for Fiscal Year 2025 Was Effective

EVALUATION REPORT

Department of Energy
Washington, DC 20585

February 6, 2026

MEMORANDUM FOR THE EXECUTIVE DIRECTOR, FEDERAL ENERGY REGULATORY COMMISSION

SUBJECT: Evaluation Report: *The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program for Fiscal Year 2025 Was Effective*

The attached report discusses our evaluation of the Federal Energy Regulatory Commission's unclassified cybersecurity program for fiscal year 2025. Based on the scope of our fiscal year 2025 test work, we did not identify any weaknesses within the Federal Energy Regulatory Commission's information technology environment. As a result, our report does not include any recommendations or suggested actions related to this evaluation.

We performed this evaluation from March 2025 through November 2025 in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (December 2020). We appreciated the cooperation and assistance received during this evaluation.

Matthew D. Dove
Assistant Inspector General
for Audits
Office of Inspector General

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

DOE OIG HIGHLIGHTS

The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program for Fiscal Year 2025 Was Effective

Why We Performed This Evaluation

The *Federal Information Security Modernization Act of 2014* (FISMA) requires Federal agencies to develop, document, and implement an agency-wide information security program to ensure that information technology resources are adequately protected. FISMA mandates that each agency Office of Inspector General, or external auditor, as determined by the Inspector General, perform an annual independent evaluation of the agency's information security program and practices to determine its effectiveness.

As an independent agency within the Department of Energy, the Federal Energy Regulatory Commission (FERC) is mandated to comply with FISMA. Therefore, we initiated this evaluation to determine whether FERC's unclassified cybersecurity program adequately protected data and information systems in accordance with FISMA. The Office of Inspector General contracted with KPMG LLP to assist in the assessment of FERC's unclassified cybersecurity program. The Office of Inspector General monitored KPMG LLP's work to ensure it complied with applicable requirements.

What We Found

Our fiscal year 2025 evaluation found that FERC had adequately protected data and information systems in accordance with FISMA. Specifically, during our review of the FISMA security metrics, we determined that FERC had implemented an effective unclassified cybersecurity program within the context of the maturity model. In addition, based on our limited testing of general information technology controls and business process application controls at FERC, we determined that all selected controls were adequately designed, implemented, and operating effectively through fiscal year end.

What We Recommend

Based on our review of the required FISMA metrics and selected controls over financial processes, we did not identify weaknesses that required immediate corrective actions related to FERC's cybersecurity program. As such, we did not make any recommendations.

DOE-OIG-26-12

Table of Contents

Background and Objective

The Federal Energy Regulatory Commission's (FERC) is an independent agency within the Department of Energy that regulates key aspects of the electric, natural gas, and oil industries. Its mission is to assist customers in obtaining reliable, safe, and economically efficient energy services at reasonable costs through appropriate regulatory and market means. Some of 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 is also responsible for reviewing proposals to build liquified 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 with protecting the reliability and cybersecurity of the bulk-power system against increased and evolving cybersecurity threats that have the potential to cause widespread disruption of electric services and threaten national security. 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 requires that each agency Inspector General (IG), or designated independent external auditor, perform an annual evaluation of the agency's information security program and practices to determine its effectiveness.

Our evaluation of FERC's unclassified cybersecurity program was, in part, performed in accordance with the *FY 2025 Inspector General FISMA Reporting Metrics* (IG FISMA Reporting Metrics), which was developed by the Office of Management and Budget (OMB), the Council of the Inspectors General on Integrity and Efficiency, and other stakeholders. The guidance represents a continuation of the multi-year reporting cycle that establishes a number of core metrics[1] to be evaluated annually, with the remaining supplemental metrics[2] to be evaluated on a 2-year cycle. As illustrated in Exhibit 1, IG FISMA Reporting Metrics, there are 10 domains which align to the 6 National Institute of Standards and Technology cybersecurity framework functions.

[1] 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.
[2] Supplemental metrics are not considered a core metric but represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness. For fiscal year (FY) 2025, the supplemental metrics comprised five new metrics designed to gauge the maturity of agencies' cybersecurity governance practices and implementation of key components of zero trust architecture.

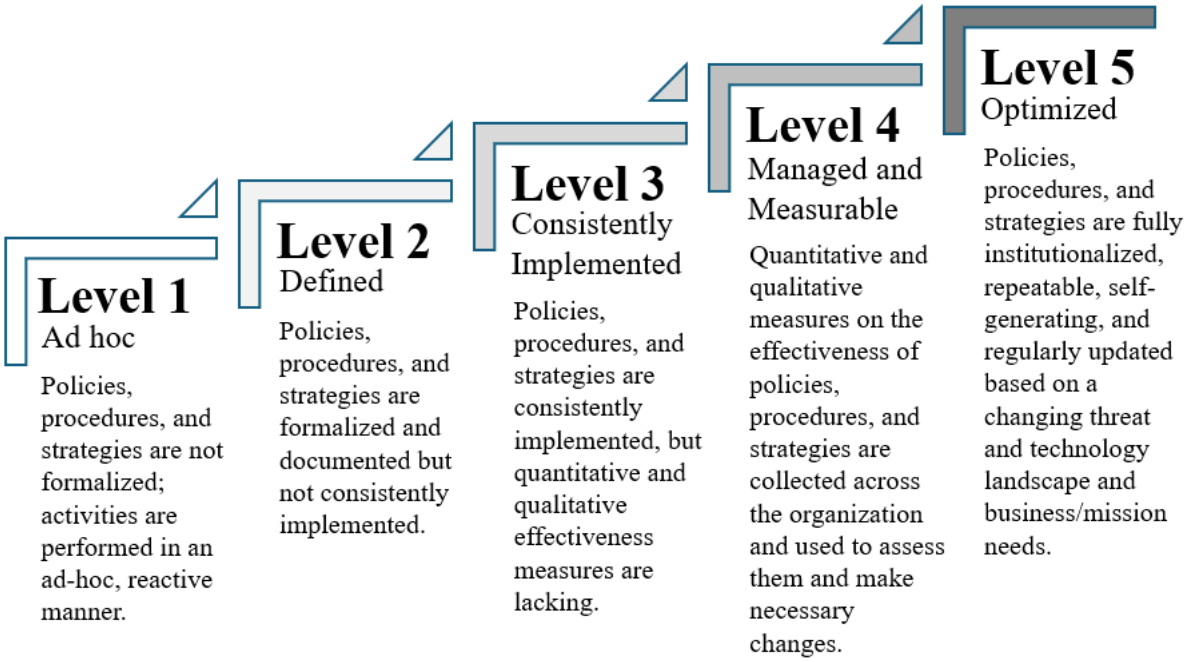
Exhibit 1: Cybersecurity Framework Functions Mapped to Metrics Assessment Domains

Cybersecurity Framework Functions	FY 2025 IG FISMA Reporting Metrics Assessment Domains
Govern	Cybersecurity Governance
	Supply Chain Risk Management
Identify	Risk and Asset Management
Protect	Configuration Management
	Identity and Access Management
	Data Protection and Privacy
	Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Source: Office of Inspector General-generated from IG FISMA Reporting Metrics.

Per IG FISMA Reporting Metrics guidance, IGs are required to assess the effectiveness of information security programs on a maturity model spectrum and report ratings and rationales to the OMB and the Department of Homeland Security. As depicted in Exhibit 2, the foundational maturity levels ensure that sound policies and procedures are developed, whereas the advanced levels capture the extent that agencies institutionalize those policies and procedures. Within the context of the maturity model, the OMB asserted that achieving a "managed and measurable" level, or above, represents an effective level of security.

Exhibit 2: IG Evaluation Maturity Levels



Source: Office of Inspector General-generated graphic based on IG FISMA Reporting Metrics.

Additionally, IGs were encouraged to evaluate the metrics based on the risk tolerance and threat models of their respective agency and to focus on the practical security impact of weak control implementations, rather than just evaluating from a compliance standpoint or mere presence or absence of controls. Furthermore, IGs were instructed to consider other data points such as:

- The results of cybersecurity audits, inspections, and evaluations conducted during the review period, to include any system security control reviews, vulnerability scanning, or penetration testing;
- The progress made by agencies in addressing outstanding IG recommendations; and
- Security incidents reported during the review period.

In response to the FISMA mandate, we initiated this evaluation to determine whether FERC's unclassified cybersecurity program adequately protected data and information systems in accordance with FISMA.

Results of Review

FERC'S UNCLASSIFIED CYBERSECURITY PROGRAM WAS EFFECTIVE

Our FY 2025 evaluation 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 OMB, and the Department of

Homeland Security. Particularly, using IG FISMA Reporting Metrics, we found that FERC achieved an "optimized" maturity level for the Protect, Detect, Respond, and Recover function areas, while the Govern and Identify function areas achieved a maturity level of "managed and measurable." As a result, we determined that FERC had an effective unclassified cybersecurity program within the context of the maturity model.

In addition, based on the testing performed during the FY 2025 FERC financial statement audit, we determined that the general information technology controls and business process application controls were adequately designed, implemented, and operating effectively through FY end. As such, we have reasonable, but not absolute, assurance of the integrity, confidentiality, and availability of data in the financial applications.

Based on the results of our evaluation, we did not identify weaknesses that required immediate corrective actions and, therefore, did not make any recommendations or suggested actions. However, our test work was limited to a review of required FISMA metrics and select controls over FERC's financial processes. Our review did not include technical vulnerability testing. (See Appendix 1 for a more detailed description of our scope and methodology).

Management Comments and OIG Response

The Federal Energy Regulatory Commission's management reviewed the draft report and did not have any comments. We appreciated the cooperation and assistance provided to us throughout this evaluation.

Objective, Scope, and Methodology

Objective

We conducted 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

We performed our evaluation from March 2025 through November 2025. KPMG LLP (KPMG), 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 six function areas in the *National Institute of Standards and Technology Cybersecurity Framework 2.0: Govern, Identify, Protect, Detect, Respond, and Recover*. In addition, KPMG reviewed FERC's implementation of FISMA. This evaluation was conducted under Office of Inspector General project number A25TG005.

Methodology

To accomplish our objective, we:

- Issued the work order to KPMG to perform several tasks including, but not limited to, a FISMA metric review and compliance with the *Federal Financial Management Improvement Act of 1996*.

- Reviewed Federal laws, regulations, and guidance related to cybersecurity (e.g., FISMA, Office of Management and Budget memoranda, and National Institute of Standards and Technology standards and guidance).

- Monitored KPMG to ensure compliance with professional standards and contractual requirements. This work included reviews of an assessment of compliance with the requirements of FISMA metrics, as established by the Office of Management and Budget, the Council of the Inspectors General on Integrity and Efficiency, and other stakeholders. In addition, we evaluated FERC's general information technology controls and business process application controls in conjunction with its annual audit of the financial statements, using work performed by KPMG.

- Reviewed prior reports issued by the Government Accountability Office and the Department of Energy Office of Inspector General relevant to the objective.

We conducted this evaluation in accordance with *Quality Standards for Inspection and Evaluation* (December 2020), issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that the evidence must sufficiently and appropriately support findings and provide a reasonable basis for conclusions. We believe that the evidence obtained

provides a reasonable basis for our findings and conclusions based on the evaluation objective. However, because our review was limited, it would not have necessarily disclosed all internal control weaknesses that may have existed at the time of our evaluation.

FERC officials waived an exit conference on January 12, 2026.

Prior Reports

Office of Inspector General

- Summary Report: *The Federal Energy Regulatory Commission's Unclassified Cybersecurity Program – 2024* (DOE-OIG-25-08, December 2024). Based on the fiscal year 2024 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 – 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.

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.

If you have comments, suggestions, and feedback on this report, please reach out at OIG.Reports@hq.doe.gov. Include your name, contact information, and the report number.

For all media-related questions, please send inquiries to OIGpublicaffairs@hq.doe.gov and include your name, contact information, and the report number.