OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

# AUDIT REPORT

DOE-OIG-19-52 September 2019

# MANAGEMENT OF CYBERSECURITY OVER SELECTED INFORMATION SYSTEMS AT DEPARTMENT OF ENERGY HEADQUARTERS

**Department of Energy**
Washington, DC 20585

September 27, 2019

MEMORANDUM FOR THE ADMINISTRATOR, ENERGY INFORMATION ADMINISTRATION
CHIEF INFORMATION OFFICER
ACTING CHIEF FINANCIAL OFFICER

Sarah B. Nelson

FROM: Sarah B. Nelson
Assistant Inspector General
for Technology, Financial, and Analytics
Office of Inspector General

SUBJECT: INFORMATION: Audit Report on "Management of Cybersecurity over Selected Information Systems at Department of Energy Headquarters"

The Department of Energy operates a variety of information technology systems and infrastructure to support its diverse missions, each of which has its own unique characteristics and demands. The Office of the Chief Information Officer (OCIO) is responsible for helping to protect the confidentiality, integrity, and availability of data and information systems operated at Department Headquarters. To aid in this effort, the OCIO manages the Energy Information Technology Services to support program and staff offices at Headquarters and select field sites. While the OCIO is the primary entity responsible for information technology operations at Headquarters, several other program offices also have significant information technology investments and resources at that location.

The *Federal Information Security Modernization Act of 2014* requires each Federal agency to develop, document, and implement an enterprise-wide cybersecurity program to protect systems and data that support the operations and assets of an agency. However, prior Office of Inspector General reports have highlighted cybersecurity weaknesses across the Department, including various types of weaknesses at Headquarters. Furthermore, the Office of Inspector General received an allegation that software and hardware utilized by the OCIO had no manufacturer support or updates/patches, which presented a security risk to the Department. We initiated this audit to determine whether the Department managed cybersecurity over selected Headquarters information systems in accordance with Federal and Department requirements.

We found the Department had not fully managed cybersecurity for selected Headquarters information systems in accordance with Federal and Department requirements. In particular, our testing of three information systems managed by the OCIO, Energy Information Administration, and the Office of the Chief Financial Officer identified weaknesses related to system and information integrity, system and services acquisition, security planning, access controls, and configuration management.

The issues we identified occurred, in part, because of various program-specific internal control weaknesses related to each of the information systems reviewed. For instance, we determined that the OCIO lacked sufficient controls to ensure that offices entered complete and accurate data into a system reviewed. Officials also had not implemented adequate acquisition controls related to planning to ensure that only the number of software licenses necessary were purchased. In addition, we found that the weaknesses related to the Energy Information Administration system reviewed occurred because of cybersecurity employee turnover within the organization and a lack of finalized policies and procedures to ensure that security updates and patches for known software vulnerabilities were applied in a timely manner. Furthermore, our test work indicated that Office of the Chief Financial Officer officials had not ensured that all appropriate technical controls were implemented to prevent or detect unauthorized changes in accordance with procedures, resulting in weaknesses with the system reviewed.

Without improvements, the systems reviewed and the data they contain will continue to be at a higher-than-necessary risk of compromise, loss, or modification. To help improve the management of the Department's cybersecurity program, we issued a detailed report to the OCIO, Energy Information Administration, and the Office of the Chief Financial Officer that included six recommendations. Management concurred with the recommendations and indicated that corrective actions were underway or planned to mitigate the findings identified in the report.

Due to the sensitive nature of the vulnerabilities identified during our audit, the report issued to the Department was for Official Use Only. We provided OCIO, Energy Information Administration, and Office of the Chief Financial Officer officials with detailed information regarding vulnerabilities that we identified.

I would like to thank all participating Department elements for their courtesy and cooperation during the review.

cc: Deputy Secretary
Chief of Staff
Chief Information Officer

Report Number: DOE-OIG-19-52