OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

AUDIT REPORT

DOE-OIG-19-42

July 2019

MANAGEMENT OF A DEPARTMENT OF ENERGY SITE CYBERSECURITY PROGRAM

Department of Energy
Washington, DC 20585

July 19, 2019

MEMORANDUM FOR THE PRINCIPAL DEPUTY ASSISTANT SECRETARY FOR ENVIRONMENTAL MANAGEMENT

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

SUBJECT: INFORMATION: Audit Report on "Management of a Department of Energy Site Cybersecurity Program"

Public Law enacted by Congress required the Department of Energy to solidify and dispose of radioactive waste, decommission the facilities used in this process, and return control of the site to the state of record. To support its environmental cleanup mission, the site reviewed uses various types of information systems that include network devices and applications to support human resources, contracting/procurement, financial and information management, logistics, and environmental management. Cybersecurity oversight is provided by the Office of Environmental Management's Consolidated Business Center. 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, including those provided or managed by contractors. We initiated this audit to determine whether the site managed its cybersecurity program in accordance with Federal and Department requirements.

The site had not fully implemented its cybersecurity program in accordance with Federal and Department requirements. We identified weaknesses related to vulnerability and configuration management, logical and physical access controls, contingency planning, and continuous monitoring. The weaknesses identified occurred, in part, because site cybersecurity officials had not ensured that requirements related to areas such as vulnerability and configuration management and other related continuous monitoring activities were fully implemented. In addition, detailed performance metrics were not in place to incentivize the site operating contractor to ensure that fully effective cybersecurity practices were implemented. Furthermore, we found that limited cybersecurity resources at the site impacted the ability of the site to ensure that all security controls were fully implemented. As a result, the integrity, confidentiality, and availability of systems and data managed by the site may be impacted by the vulnerabilities identified during our review.

To help improve the management of the site's cybersecurity program, we issued a detailed report to the site's Director that included three recommendations. Management concurred with the recommendations and indicated that corrective actions were 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 site and program 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-19-42