OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

EVALUATION REPORT

DOE-OIG-20-47

July 2020

SECURITY OVER INFORMATION TECHNOLOGY PERIPHERAL DEVICES AT SELECT OFFICE OF SCIENCE LOCATIONS

Department of Energy
Washington, DC 20585

July 6, 2020

MEMORANDUM FOR THE UNDER SECRETARY FOR SCIENCE

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

SUBJECT: INFORMATION: Evaluation Report on the "Security over Information Technology Peripheral Devices at Select Office of Science Locations"

A peripheral device is not part of the core elements of a computer but can include items such as replication devices (e.g., printers and scanners) and portable storage components (e.g., thumb drives and external hard drives). Peripheral devices are regularly connected to organizational networks and can be used to process, store, or transmit information and data. Therefore, appropriate security controls and practices should be implemented to mitigate the risks associated with the use of peripheral devices and to protect sensitive information that the devices store and process. Without adequate controls, connected devices could be used to introduce viruses or malware to the network, inadvertently expose sensitive information, be subject to loss or theft, or allow unauthorized access to networks or data.

To address emerging risks, the Office of the Chief Information Officer issued *DOE Information Technology and Cybersecurity Policy Memorandum: Removable Media Security* (DOE ITC 18-03) in May 2018, which established new standards, principles, and practices for all Department of Energy elements. We conducted our evaluation to determine whether the Department's Office of Science (Science) secured information technology peripheral devices in accordance with Federal and Department requirements. Our review focused on technical and policy controls for the following types of peripheral devices: printers, scanners, copiers, fax machines, Voice over Internet Protocol phones, thumb drives, and external hard drives.

Our evaluation of peripheral devices at four Science locations identified weaknesses related to access controls and configuration settings. The deficiencies were similar in type to those identified in prior evaluations of the Department's unclassified cybersecurity program. For example, our review disclosed access control weaknesses at two Science locations in which peripheral devices had not been securely configured to protect against unauthorized access. In addition, none of the four sites reviewed fully implemented security standards found within the

removable media policy issued by the Office of the Chief Information Officer, including requiring that all mass storage devices provide encryption, ensuring onboard antivirus capability, and using only Government furnished devices.

The issues identified occurred, in part, because sites had not fully documented or implemented procedures to ensure that peripheral devices were appropriately secured prior to connection to the internal network environment. In addition, officials had not tested peripheral devices for vulnerabilities at an organization-defined frequency. Science officials expressed concerns with the overall process in which the Office of the Chief Information Officer issued security standards, policies, and/or directives. In addition, site officials reported several challenges that prevented full implementation of the Department's Policy Memorandum related to removable media security. For instance, an official at one site indicated that various security standards had not been met because they were either technically not feasible or extremely difficult to implement. In other instances, officials indicated that the implementation of the removable media standards would be very costly, hinder collaboration, or would likely be unjustified by the risk presented to the site.

Without improvements to ensure that updated security requirements are implemented to the extent feasible, the sites reviewed might not keep pace with the challenges facing an ever-changing cybersecurity landscape. Further, absent effective implementation of access controls, the weaknesses noted during our review could allow an attacker or malicious user to make unauthorized changes to information technology peripheral devices and disclose sensitive information. Although site officials indicated that they had implemented compensating controls to mitigate identified weaknesses, the confidentiality, integrity, and availability of systems and data could be directly impacted by the vulnerabilities discovered by our test work.

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: Chief of Staff
Chief Information Officer

Report Number: DOE-OIG-20-47

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.