U.S. DEPARTMENT OF ENERGY

Office of Inspector General

DOE-OIG-26-09

January 22, 2026

Improvements Needed to Address the Department of Energy's Exposure to Information Technology Supply Chain Risks

AUDIT REPORT

Department of Energy
Washington, DC 20585

January 22, 2026

MEMORANDUM FOR THE UNDER SECRETARY FOR NUCLEAR SECURITY AND NATIONAL NUCLEAR SECURITY ADMINISTRATION; UNDER SECRETARY FOR SCIENCE; ASSISTANT SECRETARY, OFFICE OF ENVIRONMENTAL MANAGEMENT; AND CHIEF INFORMATION OFFICER

SUBJECT: Audit Report: *Improvements Needed to Address the Department of Energy's Exposure to Information Technology Supply Chain Risks*

The attached report discusses our review of the Department of Energy's information technology supply chain risk management program. This report contains two suggestions that, if fully implemented, should enhance the Department's implementation of an information technology supply chain risk management process. These suggestions should help address the Department's exposure to potentially malicious, counterfeit, or vulnerable information technology equipment or services.

We conducted this audit from September 2022 through March 2025 in accordance with generally accepted government auditing standards. We appreciated the cooperation and assistance received during this audit.

Sarah Nelson
Assistant Inspector General
for Management
Performing the Duties of the Inspector General
Office of Inspector General

cc: Deputy Secretary
Chief of Staff

DOE-OIG-26-09

DOE OIG HIGHLIGHTS

Improvements Needed to Address the Department of Energy's Exposure to Information Technology Supply Chain Risks

Why We Performed This Audit

There continues to be an increased focus on supply chain risks in the Federal Government. In December 2020, the Government Accountability Office reported that a majority of the 23 agencies reviewed, which included the Department of Energy, had not implemented selected foundational practices for managing information and communications technology supply chain risks. In the Department's case, information technology (IT) supply chain risk management (SCRM) is a particular challenge due to the diversity of its missions and decentralized operating environment.

We initiated this audit to determine whether the Department effectively managed its IT SCRM process.

What We Found

We determined that the Department made progress in effectively managing its IT SCRM process, but opportunities for improvement existed to help ensure compliance with Federal and Department requirements. Specifically, we found issues related to the accuracy of the Department's critical software inventory and insufficient assessments and reviews of potentially vulnerable suppliers. For example, the Department had not developed an accurate inventory of its critical software, which could have prevented it from protecting critical software, platforms, and data from unauthorized access. The Department also faced unknown SCRM risks because it did not always conduct assessments of technology acquisitions, including vendors with foreign ownership, control, or influence.

Without improvements to its SCRM process, the Department is vulnerable to potentially malicious, counterfeit, or vulnerable IT equipment or services. The inability to identify critical software quickly also places the Department at an elevated risk in the event of a compromise as it may be unable to rapidly respond to remediate vulnerabilities. Further, had entities routinely performed SCRM assessments and reviews, they may have increased awareness of supply chain risks involving certain vendors, resulting in different security decisions including implementing monitoring, conducting routine reviews of the vendor, or selecting a different vendor.

What We Suggest

We suggest that the Department develop an accurate inventory of its critical software. In addition, we also suggest that three of the sites reviewed ensure that policies and procedures related to SCRM for IT acquisitions are developed and effectively implemented.

DOE-OIG-26-09