GAO Highlights

Highlights of GAO-22-103441, a report to the Chairman, Committee on Homeland Security, House of Representatives

July 2022

PREVENTING A DIRTY BOMB

Vulnerabilities Persist in NRC's Controls for Purchases of High-Risk Radioactive Materials

Why GAO Did This Study

Radioactive materials are commonly used throughout the U.S. in technological devices for medical, industrial, and research purposes. However, these materials, if used improperly, can be harmful and dangerous. For example, in the hands of terrorists, even a small amount could be used to construct a radiological dispersal device, also known as a dirty bomb. A dirty bomb uses conventional explosives to spread radioactive material.

GAO was asked to review NRC's license verification system for high-risk radioactive materials. This report examines (1) the effectiveness of NRC's license verification system for ensuring that high-risk radioactive materials are not purchased using a forged or altered license and (2) vulnerabilities that could affect NRC's ability to verify licenses for the purchase of high-risk radioactive material. GAO conducted a covert investigation of controls on purchasing radioactive materials. Additional details on GAO's covert testing will be included in an Official Use Only version of this report that will be issued soon.

What GAO Recommends

GAO recommends that NRC (1) immediately require vendors to verify category 3 licenses with the appropriate regulatory authority and (2) add security features to its licensing process that improve the integrity of the process and make it less vulnerable to altering or forging licenses. To address our recommendations, NRC proposed a rulemaking to strengthen licensing. However, vulnerabilities will remain until NRC implements the rule.

View GAO-22-103441. For more information, contact Allison Bawden at (202) 512-3841 or bawdena@gao.gov or Howard Arp at (202) 512-5222 or arpj@gao.gov.

What GAO Found

The Nuclear Regulatory Commission's (NRC) current system for verifying licenses does not adequately protect against the purchase of high-risk radioactive materials using a fraudulent license. Licenses control the type and quantity of radioactive material allowed to be possessed. Quantities of radioactive materials are defined as category 1 through 5, with 1 being the most dangerous. Using shell companies with fraudulent licenses, GAO successfully purchased a category 3 quantity of radioactive material of concern from two different vendors in the U.S. Specifically, GAO provided a copy of a license that GAO forged to two vendors, subsequently obtained invoices, and paid the vendors. GAO refused to accept shipment at the point of delivery, ensuring that the material was safely and securely returned to the sender.

As GAO has previously reported, a category 3 quantity of radioactive material can, on its own, result in billions of dollars of socioeconomic costs if dispersed using a dirty bomb. By purchasing more than one shipment of a category 3 quantity of radioactive material, GAO also demonstrated that a bad actor might be able to obtain a category 2 quantity by purchasing and aggregating more than one category 3 quantity from multiple vendors. NRC officials told GAO that NRC plans to proceed with existing initiatives to implement new verification regulations by late 2023 but does not plan to take immediate corrective actions to address the issues that GAO found.

Radioactive Material Delivered to GAO's Shell Company (box on left)

Source: GAO. | GAO-22-103441

NRC requires a valid license to possess category 3 quantities of radioactive material, but the paper licenses it issues can be altered and used to make illicit purchases of radioactive materials. During this investigation, GAO created forged licenses to facilitate purchases. GAO's shell companies were successful in acquiring the material because they are not subjected to more stringent controls required for purchases of larger quantities of material. GAO's investigation demonstrates that the integrity of NRC's current license verification processes can be compromised.