United States Government Accountability Office

Testimony

Before the Homeland Security and Governmental Affairs Committee, U.S. Senate

For Release on Delivery
Expected at 10:30 a.m. ET
Thursday, June 12, 2014

NUCLEAR NONPROLIFERATION

Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources

Statement of David Trimble
Director, Natural Resources and Environment

Chairman Carper, Ranking Member Dr. Coburn, and Members of the Committee:

I am pleased to be here today to discuss the challenges federal agencies face in securing industrial radiological sources. The Nuclear Regulatory Commission (NRC) plays an important role in licensing and regulating the security of radiological sources in the United States. In addition, 37 states are responsible for implementing licensing programs, including security inspections, for industrial radiological sources. These states are referred to as "Agreement States."[1] The National Nuclear Security Administration (NNSA) provides security upgrades to U.S. facilities with high-risk radiological sources beyond what NRC requires. In addition to NRC and NNSA, the Department of Homeland Security (DHS) is the primary federal agency responsible for implementing domestic nuclear detection efforts. My remarks today are based on our report that is being released at this hearing, entitled *Nuclear Nonproliferation: Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources*.[2]

Radioactive material is used worldwide for legitimate commercial purposes, including industrial processes in the oil and gas, aerospace, and food sterilization sectors. It is typically sealed in a metal capsule, such as stainless steel, titanium, or platinum, to prevent its dispersal and is commonly called a sealed source.[3] Some of these sources are highly radioactive and are found in a variety of devices, ranging from mobile industrial radiography sources containing hundreds of curies of iridium-192 to larger irradiators with thousands, or even millions, of curies of cobalt-60.[4] In the hands of terrorists, these sources could be used to produce a simple and crude, but potentially dangerous weapon known as a radiological dispersal device or dirty bomb, whereby conventional explosives are used to disperse radioactive material.

The potential vulnerability of radiological sources was highlighted in December 2013 when a truck in Mexico carrying a cobalt-60 source was

[1]42 U.S.C. § 2021(b) (2013).

[2]GAO, *Nuclear Nonproliferation: Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources,* GAO-14-293 (Washington, D.C.: June 6, 2014).

[3]Such material includes americium-241, cesium-137, cobalt-60, and iridium-192.

[4]A curie is a unit of measurement of radioactivity.

stolen. Although the source was recovered 2 days later, NNSA officials said that the container housing the source was opened by the thieves, and NNSA was uncertain whether the intended target was the truck or the radiological source.

The threat of an individual stealing a radiological source includes both an outsider and insider threat. According to the Federal Bureau of Investigation's (FBI) website, a company can often detect outsiders (i.e., nonemployees) and mitigate the threat of them stealing company property. However, the individual who is harder to detect is the insider—the employee with legitimate access.

The security of radiological sources in the United States has been a focus of our work over the past several years, and we have reported on the challenges federal agencies face in ensuring their security and have recommended specific actions to address them. Specifically, in September 2012,[5] we reported that, at the 26 selected hospitals and medical facilities we visited, NRC's controls did not consistently ensure the security of high-risk radiological sources.

In this context, my testimony today summarizes the findings from our most recent report on industrial radiological security in the United States. Accordingly, this testimony addresses (1) the challenges in reducing the security risks posed by high-risk industrial radiological sources and (2) the steps federal agencies are taking to ensure that high-risk industrial radiological sources are secured.

For our report, we visited 33 industrial facilities in the United States.[6] We also reviewed laws, regulations, and guidance related to the security of industrial radiological sources and interviewed agency officials at NRC, NNSA, and DHS. Additional information on our scope and methodology is available in our report. Our work was performed in accordance with generally accepted government auditing standards.

[5]GAO, *Nuclear Nonproliferation: Additional Actions Needed to Improve Security of Radiological Sources at U.S. Medical Facilities,* GAO-12-925 (Washington, D.C.: Sept. 10, 2012).

[6]These facilities included, among others, industrial radiography companies, commercial or sterilization companies, academic research facilities, and well logging companies.

Challenges Exist in Reducing Security Risks for Different Types of Industrial Radiological Sources and from Insider Threats

We identified two main types of industrial radiological sources during the course of our review—mobile and stationary sources—that pose security challenges, even when licensees follow NRC's security controls. In addition, licensees also face challenges in determining which employees are suitable for trustworthiness and reliability (T&R) certification to mitigate the risk of an insider threat.

Mobile Sources. The portability of some radiological sources makes them susceptible to theft or loss. For example, the most common mobile source, iridium-192, is contained inside a small device called a radiography camera. The risks associated with mobile sources are underscored by a series of incidents involving both theft and unauthorized individuals attempting to gain access to the sources. We also identified cases of individuals impersonating state radiological safety and security inspectors at remote worksites where the mobile sources were being used.

Regarding the theft of sources, we found, for example, that a radiography camera containing about 34 curies of iridium-192 was stolen from a truck parked in a hotel parking lot. Although the door to the truck's darkroom was locked and the device secured using cables and padlocks, the truck's alarm system was not activated. The radiological source was never recovered.

Concerning individuals impersonating safety and security inspectors, we found that a radiography crew was approached at a temporary worksite by an individual who identified himself as an inspector. The individual became confrontational with the crew. The radiographers asked the individual to provide identification, but he refused and later left the worksite. The individual was identified as having multiple convictions on his record, including assault, forgery, and terroristic threats.

According to NRC officials, the agency's controls provide licensees with flexibility to meet the security requirements. NRC's security controls call for two independent physical measures—such as two separate chains or steel cables locked and separately attached to the vehicle—when securing a mobile device containing a high-risk source to a truck. The controls also call for licensees to maintain constant control and/or surveillance during transit, as well as disabling the truck containing such devices when not under direct control and constant surveillance by the licensee.

Stationary Sources. Securing stationary high-risk radiological sources also poses challenges for licensees. These types of facilities include aerospace manufacturing and research plants, storage warehouses, and panoramic irradiators used to sterilize industrial products.

One facility we visited met NRC's security controls but still had potential security vulnerabilities. Specifically, at the facility, we observed a cesium-137 irradiator with approximately 800 curies that was on wheels and in close proximity to a loading dock rollup door that was secured with a simple padlock.

NRC's security controls for stationary sources provide a general framework that is implemented by the licensee. However, the security controls are broadly written and do not provide specific direction on the use of cameras, alarms, and other relevant physical security measures.

Insider Threats. Licensees of mobile and stationary radiological sources face challenges in determining which of their employees are suitable for T&R certification, as required by NRC's security controls. Such certification allows for unescorted access to high-risk radiological sources. Under NRC's security controls, it is left to the licensee to decide whether to grant employees unescorted access, even in cases where an individual has been indicted or convicted for a violent crime or terrorism. Moreover, in such cases, the licensee is not required to consult with NRC before granting such access.

We found two cases where employees of industrial radiographers were granted unescorted access despite having serious criminal records. In one of the cases, a T&R official told us that she granted unescorted access to an individual in 2008 with an extensive criminal history, some of which was included on the FBI report the company received from NRC, and some that was absent. This criminal history included two convictions for terroristic threats that occurred in 1996, which were not included in the background information provided to the T&R official by NRC. The NRC officials said that the person was convicted not of a threat against the United States, but of making violent verbal threats against two individuals. Based on available documents, we identified that the individual had been arrested and convicted multiple times from 1996 to 2008, including for the following: assault, forgery, failure to appear in court, driving while intoxicated, driving with a suspended license, and terroristic threats (twice).

According to NRC officials, identification of a criminal history through the FBI or a discretionary local criminal history check does not automatically indicate unreliability or untrustworthiness of an individual. The licensee may authorize individuals with criminal records for unescorted access to radioactive materials notwithstanding the individual's criminal history.

Nonetheless, in the report being released today, we recommended that NRC assess the T&R process to determine if it provides reasonable assurance against insider threats. NRC acknowledged the merits of our recommendation and is planning to reevaluate this issue as part of its review of the effectiveness of the recently issued security regulations under 10 C.F.R. Part 37. This review is expected to occur 1 to 2 years after the regulations are implemented. As we noted in our report, we believe that this review should be conducted with a greater sense of urgency.

Federal Agencies Are Taking Steps to Improve Security of Radiological Sources but Are Not Always Effectively Collaborating

Federal agencies are taking steps to better secure industrial radiological sources. For example, NRC has been developing a Best Practices Guide and NNSA has two initiatives to improve industrial radiological source security. However, NRC, NNSA, and DHS—agencies that play a role in nuclear and radiological security—are not always effectively collaborating to achieve the common mission of securing mobile industrial sources.

Best Practices Guide. At the time of our review, NRC was developing a Best Practices Guide for licensees of high-risk radiological sources in response to a recommendation in our September 2012 report.[7] According to NRC officials, the guide includes information for licensees on physical barriers; locks; monitoring systems, such as cameras and alarms; as well as examples of how to secure mobile sources and sources in transit. NRC told us that during development of the Best Practices Guide they relied on a working group to provide insight into challenges licensees face in complying with NRC's security controls. However, NRC also told us that they had not directly reached out to licensees during the development of the guide to obtain the views of key stakeholders.[8]

[7]GAO-12-925.

[8]GAO-14-293.

We recommended in our report that NRC obtain the views of key stakeholders and licensees during the development of the Best Practices Guide. NRC agreed with our recommendation.

NNSA Efforts to Address Security Risks. NNSA has two initiatives under way to address security risks posed by industrial radiological sources: (1) testing and developing tracking technology for mobile sources, and (2) upgrading the physical security of industrial facilities.

Agencies Not Always Collaborating Effectively. Although DHS, NNSA, and NRC have an interagency mechanism for collaborating on, among other things, radiological security, they were not always doing so effectively. For example, we found that DHS contracted with Sandia National Laboratories in October 2011 to study commercially available technologies for tracking mobile radiological sources. DHS collaborated with NRC and several Department of Energy national laboratories to develop the study but did not share the results with key NNSA officials who are directly involved in radiological source security. NNSA is also developing a tracking system for devices containing mobile radiological sources, such as radiography cameras. However, we found that NNSA has not been collaborating with DHS and NRC on the project.

We also recommended that NNSA, NRC, and DHS review their collaboration mechanism for opportunities to enhance it, especially in the development of new technologies. NRC and NNSA agreed with this recommendation, and DHS had no comments on our report.

Chairman Carper, Ranking Member Dr. Coburn, and Members of the Committee, this concludes my prepared statement. I would be pleased to answer any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff members have any questions concerning this testimony, please contact me at (202) 512-3841 or trimbled@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Other individuals who made key contributions include Glen Levis, Assistant Director; Jeffrey Barron, Randy Cole, John Delicath, Bridget Grimes, Karen Keegan, Rebecca Shea, and Kiki Theodoropoulos.