JUNE 12, 2014

SECURING RADIOLOGICAL MATERIALS: EXAMINING THE THREAT NEXT DOOR

U.S. SENATE, COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

ONE HUNDRED THIRTEENTH CONGRESS, SECOND SESSION

HEARING CONTENTS:

AVAILABLE WEBCAST(S):*

- *Full Committee Hearing*

COMPILED FROM:

- *http://www.hsgac.senate.gov/hearings/securing-radiological-materials-examining-the-threat-next-door*

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

Opening Statement of Chairman Thomas R. Carper
"Securing Radiological Materials: Examining the Threat Next Door"
June 12, 2014

As prepared for delivery:

A little over a year ago, the city of Boston was struck by a tragedy during the running of the 117th Boston Marathon. Two terrorists detonated pressure cooker bombs near the finish line, killing three and injuring nearly 300.

The horror of this attack will never be forgotten, but neither will the heroism that unfolded immediately afterwards. These acts of courage and selflessness saved countless lives.

Police, medical personnel, National Guardsmen, volunteers, runners and spectators all ran towards the blasts to provide immediate aid to the injured. These acts of courage and selflessness saved countless lives.

The tragic events of the 117th Boston Marathon remind us that we must constantly seek to counter the threats from homegrown terrorists and to improve our nation's ability to anticipate – and prevent – the next attack.

A dirty bomb is any kind of crude explosive device that, when detonated, disperses radiation around and beyond the blast. If a dirty bomb successfully goes off, those who survive the blast can be exposed to harmful amounts of radiation that could cause sickness or even death. Moreover, a dirty bomb could render areas uninhabitable for many years, making it a highly disruptive weapon.

If the Boston Marathon terrorists had turned their pressure-cooker bombs into dirty bombs, then the consequences of that tragic day could have multiplied by an order of magnitude. Think about that for a minute.

For instance, when those police, medical personnel, volunteers, runners and spectators all ran toward the blast to help the injured, they could have been unknowingly exposed to harmful amounts of radiological material. In many cases, this material cannot be seen, smelled, felt, or tasted. In this hypothetical, what would have been a heroic display of courage and selflessness could have quickly spiraled into a far more deadly and disruptive situation.

Today's hearing will focus on how we can ensure that this hypothetical situation never comes to pass. We will focus on the threat of a dirty bomb and specifically examine the security of radiological material here in communities across the country that can be used in a dirty bomb.

Two years ago, at the request of Senator Daniel Akaka, the Government Accountability Office (GAO) issued a report examining the government's efforts to secure radiological material in U.S. medical facilities.

GAO found that in many cases, this radiological material was all too vulnerable to theft or sabotage. Shortly thereafter, I joined Senator Akaka and Senator Casey in requesting that GAO audit the security of radiological material used at construction and industrial sites.

Unlike the radiological devices in hospitals that are stationary and large, industrial radiological sources are often found in small, highly portable devices, routinely used in open, populated areas. GAO will testify today on the security of these industrial radiological materials, but the messages from their audit are clear.

Despite government efforts, industrial radiological sources are far too vulnerable to theft or sabotage by terrorists or others wishing to do us harm. In fact, GAO found four cases where potential dirty bomb material was stolen between 2006 and 2012.

Moreover, GAO found two cases where individuals with extensive criminal histories were given unsupervised access to potential dirty bomb material. One of those individuals had been previously convicted of making "terroristic threats."

We will learn more about these vulnerabilities and what I think are some commonsense fixes from GAO, but let me just say this: we must do better. Given the consequences of a dirty bomb, there really is no excuse for the vulnerabilities identified by GAO. So I'll say it again, we must do better."

If we are to protect against the next Oklahoma City bombing, the next 9/11 or the next Boston Marathon bombing, we must stay several steps ahead of the terrorists. We must anticipate and neutralize their evolving ability to carry out terrorist plots well before they are ever conceived.

Today, we will also hear from three agencies that play a critical role in securing radiological material in the U.S. and preventing dirty bomb attacks from occurring.

###

Statement of Anne Harrington
Deputy Associate Administrator for Defense Nuclear Nonproliferation
National Nuclear Security Administration
U.S. Department of Energy
Before the
Senate Homeland Security and Government Affairs Committee
June 12, 2014

INTRODUCTION

Mister Chairman, Ranking Member Coburn and distinguished members of the Committee, thank you for giving me the opportunity to testify on the Department of Energy National Nuclear Security Administration (NNSA) efforts to enhance the security of vulnerable high-risk radioactive sources in the United States. I would like to thank you for your continued interest and leadership on this important issue of securing vulnerable radioactive sources. I would also like to thank my colleagues from the Department of Homeland Security and the Nuclear Regulatory Commission for being constructive and indispensable partners in the effort to reduce the risk of radiological incidents.

SCOPE AND THREAT

When President Obama launched the Nuclear Security Summit series in 2010, the primary focus was on permanent risk reduction through the elimination of Highly Enriched Uranium (HEU) and plutonium. In the wrong hands, these materials could be used in an improvised device that would have catastrophic impact. As you know, the United States, working in concert with other countries has made very significant progress in this area. For instance, these efforts have resulted in the removal or disposition of more than 2,600 kilograms of HEU and plutonium since 2010, more than enough material for 100 nuclear weapons, which includes the removal of all HEU from eight countries. Although we still have large amounts of both HEU and plutonium to remove or secure worldwide, we have for years also engaged in parallel efforts to secure high-risk radioactive sources.

One of the missions of NNSA's Office of Defense Nuclear Nonproliferation (DNN) is to reduce and protect vulnerable nuclear and radioactive material at civilian sites worldwide, primarily through the Global Threat Reduction Initiative (GTRI) program. A key goal of that program is to enhance the security of high-risk radioactive materials that could be used in a Radiological Dispersal Device (RDD) – commonly known as a "dirty bomb." An RDD detonated in a major metropolitan area could result in economic costs in the billions of dollars as a result of evacuations, relocations, cleanup, and lost wages. Radioactive sources such as Cobalt, Cesium, Americium, and Iridium are used worldwide for many legitimate purposes and are located at thousands of sites in the United States and around the world. Since many of the sites that use these materials, such as medical, university, research, and industrial facilities are open environments, these facilities are more vulnerable to adversaries that may target these materials and are more difficult to secure. In looking at the risk, we must include not only outside terrorists attempting to steal radioactive sources as potential adversaries, but also insiders who work at these facilities who could have intimate knowledge of security procedures and vulnerabilities.

The 2014 Nuclear Security Summit Communique signed by 53 countries including the United States ". . . sets out a new ambition to secure all radioactive sources, such as those in industry, medicine, agriculture or research."[1] In addition, the importance of securing high-risk radioactive sources was highlighted at the 2014 Nuclear Security Summit[2] when 22 additional countries signed onto a United States sponsored "gift basket" committing to secure all IAEA Category I radioactive materials consistent with the IAEA's Code of Conduct on the Safety and Security of Radioactive Sources, and, where possible, to exceed those guidelines by the 2016 Nuclear Security Summit.

NNSA ROLE TO REDUCE THE RADIOLOGICAL THREAT

All three agencies appearing in today's hearing play important roles in reducing the risk of radiological terrorism. DNN collaborates with federal partners to reduce the risk of terrorists acquiring the materials for an RDD. While the Nuclear Regulatory Commission (NRC) has the mandate to license and regulate the use of civilian radioactive sources, NNSA brings the science and expertise of its National Laboratories to develop innovative solutions to prevent the acquisition of radioactive materials by adversaries. Laboratories from across the DOE/NNSA complex bring the experience of work overseas and domestically to identify and implement security best practices.

To address the risks of terrorists or other adversaries acquiring radioactive sources, DNN, in cooperation with its federal partners, launched a program in 2007 to implement voluntary security efforts at civilian sites in the United States that use or store high-risk radioactive materials. The program components include removal of unwanted radioactive sources, hardening kits for irradiators and other devices, facility-wide voluntary security enhancements, specialized training for security and law enforcement personnel, and tabletop exercises for first responders. These voluntary security efforts complement, but do not replace, NRC's regulatory requirements that govern domestic radiological site security.

When requested by the licensee, DNN's GTRI program assesses existing security conditions, provides recommendations on security enhancements, and when warranted, funds the procurement and installation of jointly agreed upon technical security upgrades and training to further the level of security. We consider 14 isotopes of concern above threshold quantities, and address several areas of security including detection, delay, response, and sustainability.

These voluntary security enhancement efforts have been endorsed by the NRC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the Organization of Agreement States (OAS), and the Conference of Radiation Control Program Directors, Inc.

---

[1] The Hague Nuclear Security Summit Communique.
https://www.nss2014.com/sites/default/files/documents/the_hague_nuclear_security_summit_communique_final.pdf

[2] 2014 Nuclear Security Summit; *Statement on Enhancing Radiological Security*.
https://www.nss2014.com/sites/default/files/documents/statement_on_enhancing_radiological_security_final_version_of_24_march2.pdf

(CRCPD). NRC has issued Regulatory Information Summaries (RIS) describing these voluntary security enhancement initiatives and recommends that licensees volunteer for these DNN-GTRI efforts.[3]

DNN prioritizes which sites receive voluntary security enhancements by assessing the attractiveness of the site's materials for possible use in an RDD, the site's proximity to DHS Urban Area Security Initiative (UASI) locations, and the site's proximity to other volunteer sites. We estimate that there are about 3,000 buildings in the United States that house high-risk radioactive materials. As of May 31, 2014, security enhancements and training for 1,742 buildings have been completed.

Consistent with U.S. commitments at the 2014 Nuclear Security Summit, DNN will prioritize its work at sites containing IAEA Category I materials. All Category I buildings in the United States currently meet NRC regulations and the international guideline. However, DNN's GTRI program has provided additional voluntary security enhancements that build on this standard to 273 of 554 Category I sites and will reach out to the remaining 281 sites with the goal of completing security enhancements by 2016. Additional security enhancements include In-Device Delay (IDD), Remote Monitoring Systems (RMS), and promotion of an adequately trained response force that can prevent an adversary from stealing high-risk radioactive materials.

Elimination – Removing Unwanted Sources

Since 1997, DOE/NNSA's Off Site Source Recovery Project (OSRP) operated by Los Alamos National Laboratory, Idaho National Laboratory, and the CRCPD has reduced the radiological risk by recovering and eliminating disused and unwanted sealed sources. DNN, in coordination with NRC, developed recovery prioritization criteria based on risk reduction. As of May 31, 2014, DOE/NNSA has recovered over 36,000 sources.

Irradiator In-Device Delay (IDD)

A fundamental component of our voluntary security enhancement program is delay. By increasing delay (the amount of time needed by the adversary to gain access to the radioactive sources) we give more time for law enforcement to interrupt the adversary before they can steal the radioactive source. As a result of the interagency DNN /DHS Domestic Nuclear Detection Office (DNDO) cesium irradiator vulnerability study, which utilized input from the three main cesium irradiator manufacturers IDD hardening kits were developed for the most widely used models of Cesium blood and research irradiators. These IDD kits increase the difficulty for an adversary to illicitly access and steal the radioactive source.

In August 2008 the IDD kit designs were completed. The NRC and corresponding Agreement States reviewed the designs and authorized the launch of a voluntary pilot program to install the

[3] RIS 2010-02; NRC Regulatory Issue Summary 2010-02 The Global Threat Reduction Initiative (DNN) Federally Funded Voluntary Security Enhancements for High-Risk Radiological Materiel, January 21, 2010; http://pbadupws.nrc.gov/docs/ML1001/ML100150354.pdf

first IDD kits. The pilot effort was deemed a success and DNN has initiated a national implementation plan to outfit all qualifying irradiators in the United States. The total number of Cesium devices in the United States is about 1,100, of which 815 are IDD eligible at this time. Each one of these Cesium irradiators has more than enough material to be used in a significant RDD. As of May 31, 2014 IDD kits have been installed on 463 irradiators. The remaining 352 irradiators can be hardened by FY20. In addition, the manufacturers have agreed to start factory hardening, or installing IDD kits at the factory, on all new irradiator sales. DNN has expanded its IDD efforts to include devices that use Co-60

In addition to the IDD hardening kits for Cesium Chloride-based irradiators, DNN voluntary security enhancements also include other delay elements such as device tie downs, locks, hardened doors/windows, walls, cages, and safes. All of these elements increase the time it takes the adversary to gain access to the radioactive source.

Detection – Remote Monitoring

A second fundamental component of the voluntary security enhancements program is detection. Increased delay coupled with detection that allows responders to arrive prior to source removal is considered to be effective. Increased delay without detection or timely response could allow the adversary to attack the source/device all weekend and would not be sufficiently effective in providing notification to responders of an adversary attack.

DNN-GTRI supplied detection upgrades include biometric access control devices, door alarms, motion sensors, cameras, wireless electronic tamper indicating seals, and area radiation monitors. Each of these technologies provides a specific deterrence, control, and/or detection function that, when integrated together and with delay, provides a significant security enhancement in a holistic manner.

The program also deploys remote monitoring systems that provide reliable transmission of alarms to responders and addresses the insider threat. Remote monitoring systems directly mitigate the insider threat by integrating alarms from multiple detection sensors (including device tamper sensors and radiation sensors) and prioritize alarms to ensure that critical alarms receive immediate attention. Alarms are simultaneously sent to on-site and off-site locations such as local police departments, regional emergency operation centers, or security contractors. This ensures a timely response by sending a reliable transmission of alarms directly to trained off-site experts and responders and protects against a single-point failure if the insider is the on-site alarm monitor or guard.

To address the sustainability portion of our security enhancement concept, DNN provides a three to five year maintenance and warranty contract for each security enhancement device, contacts each site quarterly to follow-up on the status of the enhanced security system, and conducts one follow-on visit to determine if changes to the operating or threat environment warrant additional system enhancements.

Response – Alarm Response Training

The most important aspect of any security system is a timely, well equipped, well trained response team of appropriate size to interrupt and neutralize the adversary before they gain

access to the radioactive source. We have made a focused effort to provide security personnel and local law enforcement with the tools and training needed to adequately respond to a security incident.

Most on-site guards at facilities with radioactive sources are not armed nor do the sites have large enough force strength to neutralize the threat. Therefore, the key responders are often off-site local law enforcement. Despite regulations requiring licensees to coordinate with local law enforcement, consistent feedback received from law enforcement officials indicates that they were not aware of the nature and risks associated with the material which is in use at hospitals, blood banks, universities, oil fields and manufacturing plants in their jurisdiction. It is important for their safety, and the safety of their communities, that they receive proper training about radioactive sources, about which many misconceptions exist. To ensure that both on-site and off-site responders understand how to respond to enhanced security system alarms, we have developed an alarm response training course run by the Y-12 National Security Complex in Oak Ridge, TN. This provides a venue for licensees and law enforcement officials to be in the same room and encourages the required coordination.

This alarm response training prepares responders to protect themselves and the public when responding to events involving radioactive materials. The participants conduct hands-on training in a realistic setting using actual protection equipment and real radioactive sources. The courses include operational exercise scenarios that build on classroom instruction and allow response forces to exercise their own procedures during realistic alarm scenarios.
As of May 31, 2014, we have conducted 85 training courses for 3,226 participants from 44 states.

Table Top Exercises (TTX)

As the capstone of the voluntary security enhancement support, DNN has partnered with NNSA's Office of the Associate Administrator and Deputy Under Secretary for Counterterrorism and Counterproliferation and the FBI's Weapons of Mass Destruction Directorate to provide table top exercises at select nuclear and radiological sites. The purpose is to provide a no-fault, site-specific scenario where senior managers from various Federal, State and Municipal organizations can exercise their crisis management and consequence management skills in response to a terrorist incident. The overall objectives are:

- Promote cross-sector communication, cooperation, and team-building among Federal, State, Local, and private sector first responders;
- Exercise FBI lead responsibility for criminal investigation;
- Examine newly developed tactics, techniques, and procedures resulting from DNN voluntary security enhancements;
- Promote attack prevention through intelligence sharing and coordinated approach to neutralize the threat;
- Prepare site specific integrated response plans with Federal, State, Local, and private sector partners.

As of May 31, 2014, we have conducted 35 TTXs.

Transportation

Radioactive sealed sources may be at their most vulnerable when in transit. Recognizing this, DNN implements security upgrades beyond regulatory requirements on our own source recovery shipments. Theses security enhancements include:

- Use of the DOE Transportation Tracking and Communication System (TRANSCOM) system for continuous monitoring of shipments;
- Driver duress button provides an alert signal upon activation;
- Text based communications channel provides a secondary satellite-based communication capability between the truck crew and the monitoring center;
- Delay boxes for up to thirteen 55-gallon-drum-sized packages providing delay from a broad variety of breaching tools and tactics;
- Run-flat inserts for all tires – provides capability to operate the truck at highway speeds for up to 50 miles after a tire is flattened.

INDUSTRIAL RADIOLOGICAL SOURCES

DNN's voluntary radiological security program includes addressing the security of industrial radioactive sources such as mobile sources used for oil well logging and radiography and panoramic irradiators.

Mobile Radiography and Well Logging Sources

Oil Field Service companies and Nondestructive Testing companies use radioactive sources in their industry – well logging and radiography. Because these sources are mobile (as opposed to devices in other industries that remain geographically static in a fixed location for storage and operation), DNN is collaborating with device manufacturers and end users to build GPS-enabled tracking technologies for radiography and well logging devices, transport containers and transport vehicles, and will work to promote appropriate monitoring and response procedures.

For radiography devices DNN is working with the largest device manufacturer to develop a tracking and security solution that will be integrated into the device package itself. The security package will include tamper and radiation alarms that can be transmitted to monitoring stations. A secure storage box with tamper detection would be provided for transport of the device while in trucks. DNN will work with industry partners to seek cost sharing arrangements for the deployment of the security package once developed.

For well logging devices, DNN is working with a major oil services company to develop a tracking and security system for the source containers while in transport to the field. The security package for well logging sources will also include GPS tracking, radiation detection, and tamper detection. DNN is implementing the pilot on a cost sharing basis and it is anticipated that once the tracking system is developed, major industry partners would procure the system. DNN may need to work with smaller industry partners to procure these systems under cost sharing arrangements.

The successful deployment of tracking and security systems with well logging and radiography devices may provide a security solution for these devices in storage as well as while mobile, thus reducing the number of buildings that require comprehensive site security upgrades and enabling DNN to accelerate overall program timelines.

Panoramic Irradiators

Panoramic irradiators have the highest activity of devices that use radioactive sources containing 1 to 7 million curies of Cobalt-60. The activity in Cobalt-60 sources in panoramic irradiators accounts for over 98% of the total activity in all civilian radiation sources in the United States. Industrial panoramic irradiators are used to irradiate single-use medical devices and products, cosmetics, food, and plastics. The sealed source is contained in a storage pool and is fully shielded when not in use; the sealed source is exposed within a radiation volume that is maintained inaccessible during use by an entry control system. These panoramic irradiators require re-sourcing every 18-24 months, which involves the transport of large quantities of Cobalt-60 throughout the United States and installation of Cobalt-60 pencils in the source rack. There are two major companies which operate the majority of the more than 60 industrial panoramic irradiators in use in the United States.

Due to the complexities of designing and installing security enhancements for panoramic irradiators, DNN is implementing a pilot security project at one panoramic facility. Once the pilot is proven successful and a working security system is installed, DNN will work with the industry partners to gain buy-in for expansion of security enhancements to the other panoramic irradiator sites.

Government Accountability Office (GAO) RECOMMENDATIONS

In the GAO's September 2012 report on Security of Radiological Medical Sources[4], the GAO recommended that NNSA increase outreach efforts to promote awareness and participation in NNSA's security program giving special attention to medical facilities with high-risk radioactive sources located in or in close proximity to urban areas. NNSA DNN has developed a strategy to further enhance its outreach efforts by:

- Accelerating and expanding outreach activities in conjunction with State regulators in states with the most IAEA Category I sites remaining, including Georgia, Florida, Wisconsin, Illinois, Texas, and California;
- The development and issuance of publications on DNN Security Recommendations for Users of Radioactive Sources and Security by Facility Design;
- Assisted NRC in creation of its security best practices guide.

The GAO's Draft May 2014 report on Security of U.S. Radiological Sources included a recommendation to NNSA stating "to better leverage resources, including expertise, to address

[4] GAO-12-925, United States Government Accountability Office, *Nuclear Nonproliferation: Additional Actions Needed to Improve Security of Radiological Sources at U.S. Medical Facilities*. http://www.gao.gov/products/GAO-12-925

vulnerabilities with radioactive sources while in transit, we recommend that the Administrator of NNSA, the Chairman of the NRC, and the Secretary of DHS review their existing collaboration mechanism for opportunities to enhance collaboration, especially in the development and implementation of new technologies."[5]

In implementing voluntary security enhancements at sites with radioactive sources, NNSA has maintained close coordination and cooperation with Federal, State, and local agencies and the private sector. In particular, we have established strong working relationships with the NRC, DHS, and the FBI.

To coordinate these complementary efforts, DNN participates regularly in meetings of the DHS-chaired Nuclear Sector Government Coordinating Council, the NRC-led Radiation Source Protection and Security Task Force, tri-lateral meetings comprised of senior representatives from NNSA, DHS, FBI, and NRC, and many additional working level meetings. These coordination venues have helped communicate to officials throughout the government so that they are aware of new initiatives, ongoing implementation efforts, and challenges encountered with enhancing radioactive source security.

In response to the GAO's recommendation, NNSA will continue to seek opportunities to further enhance coordination. DNN has recently briefed DNDO on its material tracking technology plans, has provided briefings on DNN RDD studies, and is jointly exploring options to enhance collaboration on response training and exercises.

STRATEGY FOR PERMANENT THREAT REDUCTION

While DNN continues to proceed with implementation of security enhancements for high-risk radioactive materials, several factors led DNN to consider a new strategic approach to addressing the RDD threat through actions that achieve permanent and sustainable threat reduction. These factors include the large number of radioactive sources worldwide, the ongoing production of new devices with radioactive sources, and the long-term costs for sustaining security systems.

DNN is developing a broader strategic approach to achieve more permanent risk reduction for vulnerable radioactive materials that will complement the existing removal project. The centerpiece of this strategy is to lead a worldwide effort to provide reliable non-radioactive alternatives for the highest activity radioactive sources that pose the greatest risk. DNN will promote the conversion or replacement of devices that use radioactive materials to non-radioactive material devices, thereby removing certain risk of an RDD threat to the United States and worldwide. DNN is considering the provision of incentives for replacement where commercially viable alternatives exist and is collaborating with Defense Nuclear Nonproliferation's Research and Development Office to explore and assess technological improvements that could be developed and ultimately transferred to industry for commercialization where necessary.

[5] GAO-14-203 DRAFT, United States Government Accountability Office, *Nuclear Nonproliferation: Additional Actions Needed to Increase Security of U.S. Industrial Radiological Sources*.

For instance, DNN is exploring the possibility of providing incentives for replacement of Cesium irradiators with commercially available x-ray devices, which might include cost sharing for new x-ray devices along with payment for removal of the Cesium irradiator. This approach may accelerate program timelines by implementing replacements instead of enhancing security and also will achieve permanent threat reduction. DNN is exploring the feasibility of replacement options for other devices including teletherapy, radiography, and well logging.

CONCLUSION

Our efforts on radioactive security measures to reduce the risk of terrorists acquiring an RDD are vital. We will continue to seek innovative approaches to enhancing security of high-risk radioactive materials. With your continued support, NNSA will continue to work with federal and industry partners to implement security enhancements on an accelerated basis in the most cost effective manner possible.

That concludes my statement and I will be happy to respond to your questions.

Huban A. Gowadia
Before the U.S. Senate Committee on
Homeland Security and Governmental Affairs
June 12, 2014

Good morning Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. As Director of the Department of Homeland Security's (DHS) Domestic Nuclear Detection Office (DNDO), I am pleased to testify today with my distinguished colleagues to discuss efforts to prevent and prepare for radiological events.

Since its inception, DNDO has built essential partnerships, architecture, and capabilities to detect and interdict radiological and nuclear threats. My testimony today focuses on that work and our continued efforts to improve information sharing and collaboration with our state and local partners.

DNDO's Efforts to Prevent and Prepare for Radiological and Nuclear Terrorism

Radiological and nuclear terrorism remains one of the greatest threats not only to our Nation's security, but to global security. Such an attack would have profound and prolonged impacts to our Nation and to the world. DNDO works with federal, state, local, international, and private sector partners to develop the appropriate detection capabilities to prevent and prepare for radiological and nuclear events.

DNDO's focus is on detecting and reporting attempts to import, possess, store, develop, or transport radiological and nuclear material that is out of regulatory control, and may be used against the Nation. We work closely with the Nuclear Regulatory Commission and the Department of Energy (DOE), who are responsible for securing radioactive materials. Together, they are working on initiatives to improve the security of risk-significant sources. Although DNDO is not directly involved in the physical security of radioactive sources, we coordinate with federal, state, and local agencies to detect and locate materials once they are lost or stolen.

Recognizing the threat posed by radiological and nuclear materials, DNDO was created by Presidential Directives NSPD-43 and HSPD- 14. DNDO was subsequently given statutory authority by Title V of the SAFE Port Act (Pub. L. No. 109-347), which amended the Homeland Security Act of 2002. Pursuant to Section 1902 of the Homeland Security Act, along with its technical nuclear forensics mission, DNDO is required to develop, with the approval of the Secretary and in coordination with the Intelligence Community, the Departments of Energy, State, Defense and Justice, and other components within DHS and our international partners, an enhanced global nuclear detection architecture, and is responsible for implementing its domestic component. The global nuclear detection architecture is a framework for detecting, analyzing, and reporting on nuclear and other radioactive materials that are out of regulatory control. Working with our partners, DNDO conducts transformational research, development, testing, and evaluation of advanced detection technologies, measures detector system performance, and ensures effective response to detection alarms. Additionally, DNDO leads the development and implementation of the national strategic five-year plan for improving the nuclear forensic and attribution capabilities of the United States required under section 1036 of the National Defense Authorization Act for Fiscal Year 2010. Nuclear forensics serves as the technical component of

our capability to attribute nuclear events. As such, it is a keystone of the U.S. policy to hold fully accountable any state, terrorist group, or other non-state actor that supports or enables terrorist efforts to obtain or use weapons of mass destruction.

While DHS focuses on threats of all types, DNDO's sole focus is on the prevention of radiological and nuclear terrorism. To maximize the ability to detect and interdict threats, we rely on the critical triad of intelligence (including information sharing), law enforcement (including training), and technology. In doing so, we apply detection technologies in intelligence-cued searches conducted by well-trained law enforcement and public safety officials. Contributions from our state and local partners are vital to the domestic component of the global nuclear detection architecture. As such, we continue to work with them to build a flexible, multi-layered, domestic architecture based on capabilities that can be integrated with federal assets into a unified response when intelligence or information indicates a credible nuclear threat.

Intelligence and Information Exchange

The first leg of the critical triad is intelligence and information sharing, which forms the backbone of a robust detection architecture. State and major urban area fusion centers, State Emergency Control Centers, and the Federal Bureau of Investigation regional offices provide the necessary information exchange pathways. In the event of an emergency, this connected system provides federal, state, and local personnel with the ability to exchange sensitive information in a timely and secure fashion.

DHS as a whole has enhanced information sharing capabilities by:

- Improving production and dissemination of classified and unclassified information regarding threats to the Homeland;
- Continuing to improve analytic capabilities through the development of a national network of state and major urban area fusion centers so that national intelligence can be incorporated into a local context;
- Standardizing how we train state and local law enforcement to recognize indicators of terrorism-related criminal activity and report these suspicious activities to Joint Terrorism Task Forces for investigation and to fusion centers for analysis;
- Increasing community awareness and encouraging the public to report suspicious activity to local authorities;
- Deploying 70 Homeland Secure Data Network systems across the country to provide access to classified information and intelligence at the local level;
- Training state and local analysts at fusion centers to ensure they have the necessary skills and expertise to analyze and fuse intelligence and information from the Intelligence Community with local/regional context and produce relevant and timely products for their stakeholders; and

- Developing tailored product lines to meet the needs of state and local partners, and expanding the distribution of products to ensure all relevant and appropriate information is shared with state and local partners.

Joint Analysis Center

DNDO's Joint Analysis Center is also essential in enhancing situational awareness, as well as providing technical support and informational products, to federal, state, and local partners. The Joint Analysis Center utilizes a secure web-based dashboard to collaborate with mission partners and uses a geographic information system to show detection information, detectors, situational awareness reports, and other overlays in a geospatial viewer. Utilizing the Joint Analysis Center Collaborative Information System (JACCIS), DNDO facilitates nuclear alarm adjudication and the consolidation and sharing of information and databases. JACCIS provides our state and local partners with the ability to manage, document, and execute a radiological and nuclear detection program. This includes the ability for them to maintain training, certification, and Memoranda of Understanding and Memoranda of Agreement between jurisdictions. JACCIS also consolidates and maintains a database of detector equipment and Nuclear Regulatory Commission State licenses. Finally, through this information system, we connect to the Triage system, maintained by the DOE's National Nuclear Security Administration, to enable a seamless transition when national-level adjudication assistance is required.

DHS Capacity Building with Operational Partners

The second leg of the critical triad is law enforcement. DHS realizes that state and local law enforcement officers and public safety officials are on the frontline of detection and prevention efforts and we work very closely with them to ensure that they have the equipment, training, and information necessary to prevent and prepare for threats. Through Federal Emergency Management Agency grants and other DHS programs such as Securing the Cities, we have helped our state and local partners procure and deploy radiation detection equipment across the Nation. This equipment is one of the building blocks for a radiation detection program.

DHS has made considerable progress in enhancing radiation detection capabilities by:

- Engaging with 29 states to raise awareness and begin developing formal radiological and nuclear detection programs. By the end of Fiscal Year 2015, DNDO plans to expand its efforts to reach all 50 states.
- Supporting activities in the New York City/Jersey City/Newark region. Through the Securing the Cities program, DNDO has developed a robust regional nuclear detection program that serves as a model for future sites.
- Based on lessons learned in the first implementation, DNDO expanded the Securing the Cities program in Fiscal Year 2013 to the Los Angeles/Long Beach area and will select a third region in Fiscal Year 2014.

In addition, DNDO provides the ability to surge resources for use during special events, times of increased threat, or in response to information or events that indicate the need for enhanced detection capabilities. This is conducted using Mobile Detection Deployment Units, trailer-based units outfitted with an extensive suite of nuclear detection equipment and communications capabilities. These units are deployed regionally across the United States and can be deployed as needed to augment federal, state, and/or local capabilities. Each unit is configured to outfit numerous personnel and contains a number of systems that can be used in vehicle backpacks, high-resolution handheld devices, personal radiation detection devices, communications, and tracking equipment. When deployed, the unit is accompanied by technical support staff to train federal, state, and/or local personnel on the use of equipment and to help integrate these surge capabilities into other protective operations. Since 2009, DNDO has deployed the Mobile Detection Deployment Units to more than 149 special security events and exercises in support of federal, state, and local law enforcement and public safety personnel.

Training is an essential element of the law enforcement leg of the critical triad. This is particularly important since, the ability to detect illicit radiological and nuclear material is a perishable skill that must be continuously refreshed. Consequently, in addition to assisting our partners with the procurement of detection systems, DNDO supports the development and delivery of robust training programs to expand and enhance radiation detection capabilities. Through many collaborative efforts, we have provided radiation detection training to over 27,000 state and local law enforcement personnel and first responders.

A significant part of any training program includes exercises. To this end, we work with our state and local partners to design and conduct realistic exercises that provide operators with valuable hands-on experience in radiological detection operations. Annually, we conduct approximately 15 tabletop or full-scale exercises across the country that specifically stress operators' ability to detect radiological material that is out of regulatory control.

In the day-to-day work of a first responder, the occurrence of illicit radiological or nuclear incidents is rare, making training, exercises, and assessments particularly important so that individuals remain ready to react to an actual incident. This is where we bring to bear our unique red team capabilities that can challenge our operational partners with uncommon nuclear sources and scenarios. Annually, DNDO's red team conducts over 20 operations, evaluating deployed systems and operations, and their associated tactics, in as-close-to-realistic environments as possible. They utilize adversary tactics and scenarios to challenge federal, state, and local operators performing radiological and nuclear detection and interdiction operations.

New Technologies for Nuclear Detection

The final leg of the critical triad is technology. DNDO continues to develop breakthrough technologies with significant operational impacts on our national capability to detect radiological and nuclear threats. For example, DNDO led the development of next-generation radioisotope identification devices which are used by law enforcement officers and technical experts during

operations to identify radioactive material. We worked closely with U.S. Customs and Border Protection, U.S. Coast Guard, the Transportation Security Administration, and state and local operators to identify key operational requirements for the design of the new system. Based on an enhanced detection material, lanthanum bromide, and improved algorithms, this new handheld technology is easy-to-use, lightweight, and more reliable. Additionally, because it contains built-in calibration and diagnostics, it has a much lower annual maintenance cost.

Several DNDO sponsored research efforts have led to new commercial products providing federal, state, and local law enforcement and public safety personnel with enhanced operational capabilities. DNDO funded the development of Strontium Iodide and Cesium Lithium Yttrium Chloride which are radiation sensing materials with enhanced detection characteristics. Commercial product lines using these enhanced capabilities are now available, and DNDO proactively engages industry to procure commercial-off-the-shelf devices to field such new technologies for nuclear detection.

By eliminating technical risk for industry, DNDO's research in networked radiation detector systems has led to making commercial products available to responders. These networked detector systems provide operators with enhanced detection, location, and tracking abilities. DNDO also supports ground-breaking research to improve current capabilities. For example, we are developing a next generation aerial radiological detection system, the Airborne Radiological Enhanced-Sensor system. This system places highly-sensitive radiation detector arrays with a visual target tracking capability aboard a helicopter to provide responders with a significantly enhanced ability to detect threats on the ground and at sea.

DNDO has also made strides in protecting the Nation from nuclear terrorism through test and evaluation assistance. To develop effective detection programs, federal, state, and local partners require reliable information on the technical performance, operational effectiveness, and suitability of currently available nuclear detection equipment. DNDO has established a robust test and evaluation capability to rigorously assess commercially available detection systems against national and international standards and in operational scenarios. For instance, DNDO recently completed the Illicit Trafficking Radiation Assessment Program, a collaboration with the European Commission's Joint Research Center and the International Atomic Energy Association. The program tested nearly 80 available instruments against consensus standards. The testing enabled our stakeholders to compare the performance of commercially available radiation detection equipment and provided manufacturers with constructive feedback on their products.

By including operational partners in the planning and execution of test events, we ensure the equipment is tested in the manner in which it will be used. Such tests independently assess system performance and provide operational data to develop effective concepts of operation. Since inception, DNDO has conducted over 96 test campaigns that involve all classes of nuclear detection systems, including personal radiation detectors, handheld, backpack and mobile

detection systems, radiation portal monitors, and radiation detection systems suitable for maritime environments and aerial platforms. The results of these efforts are shared with operational partners to inform acquisition decisions.

Conclusion

Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee, thank you for the opportunity to discuss the ongoing efforts of DNDO to prevent and protect against radiological threats.

I appreciate your continued support as we work with our partners to make nuclear terrorism a prohibitively difficult undertaking for the adversary. By developing, evaluating, and deploying the right technologies, ensuring timely intelligence and information sharing, and regularly training and exercising with our law enforcement and public safety officials, we can effectively protect our Homeland from radiological and nuclear terrorism.

WRITTEN STATEMENT
BY MARK A. SATORIUS, EXECUTIVE DIRECTOR FOR OPERATIONS
UNITED STATES NUCLEAR REGULATORY COMMISSION
TO THE
SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
JUNE 12, 2014

Good morning Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. I appreciate the opportunity to appear before you today on behalf of the U.S. Nuclear Regulatory Commission (NRC). Today I'd like to address the NRC's activities to ensure the security of radioactive sources.

Radioactive source security has been, and continues to be, a top priority for the NRC. The NRC's efforts have been effective, keeping incidents involving radioactive sources to a minimum, and their potential consequences low. The NRC continues to work with the 37 Agreement States and domestic and international organizations on a variety of initiatives to make risk-significant radioactive sources even more secure and less vulnerable to malevolent use.

Brief History of Materials Security at NRC

The events of September 11, 2001, changed the threat environment and resulted in significant strengthening of the security of radioactive sources. While the NRC's fundamental goals to protect public health and safety, promote the common defense and security, and protect the environment, remained unchanged, the NRC recognized a need to increase its requirements for security of radioactive sources. Immediately following September 11, 2001, the NRC, working with other Federal and State agencies, prioritized actions to enhance the security of radioactive sources and facilities. These initial actions resulted in the NRC disseminating a number of security advisories to NRC and Agreement State licensees, recommending specific actions to enhance security, address potential threats, and communicate general threat information. Although these security advisories did not impose legally binding requirements, much of the regulated community understood the change in the threat environment and the need for increased security and implemented the recommended actions.

With voluntary security measures in place, the NRC proceeded with multiple activities in parallel. The NRC provided experts to serve on both national and international working groups to determine what radioactive sources needed enhanced security. The NRC staff also actively participated in studies, both domestic and international, to examine commonly used medical, academic, and industrial radioactive sources. These efforts eventually became the list of sources found in the International Atomic Energy Agency Code of Conduct on the Safety and Security of Radioactive Sources.

The NRC sought to move away from voluntary security enhancements and toward legally binding requirements subject to inspection and enforcement. As this transition occurred, the NRC recognized the need to carefully integrate this increased security with the existing regulatory structure for safety of radioactive and to ensure that security measures do not diminish safety. Together with the law enforcement and intelligence communities, the NRC staff conducted threat analyses to document the credible motivations, intentions, and capabilities of potential adversaries. The NRC also conducted facility security assessments to help inform the additional security and control measures needed to protect against the risk of malevolent use risk-significant radioactive sources. Once the NRC identified specific actions that licensees needed to take to enhance the security and control of risk-significant sources, the NRC incorporated all this information to develop requirements to improve the ability to detect, assess, and interrupt adversaries who attempt to steal, divert, or sabotage radioactive sources. These requirements included:

- Access controls, including fingerprinting and background checks for personnel with unescorted access to the sources
- Detection, assessment, and response capabilities
- Transportation controls
- Information protection

The NRC issued Orders that imposed legally binding requirements on individual licensees. The need for urgency revealed by threat assessments and facility security assessments made it essential for the NRC to act quickly to remove any security gaps by using orders, rather than the normal rulemaking process which takes longer.

In order to prioritize its work on risk significance, Orders for the most risk significant facilities, such as commercial nuclear power plants, were first issued in 2002. Orders were issued to large panoramic and underwater irradiators in June 2003, manufacturers and distributors of radioactive material in January 2004, and licensees transporting radioactive materials in July, 2005. Other risk-significant materials licensees received Orders in late 2005.

In 2005, the Energy Policy Act expanded the NRC's authority to ensure the security and control of additional risk-significant materials, and required fingerprinting and Federal Bureau of Investigation (FBI) criminal history records checks for individuals with unescorted access to risk-significant radioactive sources. This legislation also mandated the development of a national registry of radioactive sources. Accordingly, in 2007, the NRC and Agreement States issued additional security Orders to licensees requiring fingerprinting and an FBI criminal history background check on anyone with unescorted access to risk significant radioactive sources.

The Energy Policy Act of 2005 also established an interagency task force on radiation source protection and security under the lead of the NRC to evaluate and provide recommendations to the President and the Congress relating to the security of radiation sources in the U.S. from potential terrorist threats. This task force submitted its first report to the President and Congress in August 2006, concluding that there were no significant gaps in the area of radioactive source protections and security that were not already being addressed. The Task Force submitted its second report to the President and Congress in August 2010, providing an update on the progress made since the 2006 report and proposing new recommendations in an effort to continue to improve the security of radioactive sources. The Task Force will submit the third report in August, 2014.

National Materials Management Program

In late 2006 and early 2007, the U.S. Government Accountability Office (GAO) conducted a test on the NRC's controls governing the issuance of licenses for possessing certain types of radioactive sources, and for enforcing possession limits on the quantities of those materials. GAO reported that they were able to obtain radioactive sources licenses for two fictional companies, modify the licenses to raise the possession limits, and then use the augmented licenses to receive quotes for purchasing radioactive sources from legitimate licensees. GAO did not acquire the materials.

A hearing was held July 12, 2007, by the Permanent Subcommittee on Investigations of this Committee following issuance of GAO's report. At that hearing, a web-based licensing (verification) system was discussed which would allow suppliers to validate purchaser licenses, and the authorized quantity that a purchaser could obtain.

In an effort to better track transactions of radioactive sources nationally, the NRC developed a portfolio of automated tools to track credentials, inspections, devices and sources, and events, and verify licenses. This portfolio includes: the National Source Tracking System (NSTS), the Web Based Licensing (WBL) System and the License Verification System (LVS).

The NSTS allows the NRC to follow transactions of nationally-tracked, high-risk radioactive sources from origin, through transfer to another licensee, to final disposition. The WBL System assists in managing the NRC's licensing information regarding businesses that use radioactive sources. The LVS is a "national verification system" that accesses license information and ensures that only authorized licensees obtain radioactive sources in authorized amounts. These systems ensure that national radioactive source authorization, possession, and transaction information is available to all government agencies that protect the country from radiological threats; provide licensees with a secure automated means to verify license information and possession authorization prior to initiating radioactive source transfers; enable the NRC and the Agreement States to monitor the location, possession, transfer, and disposal of high-risk radioactive sources throughout the country; improve source accountability by licensees; and alert regulators to track discrepancies.

Improvements in Pre-licensing Activities

Another recommendation of the 2007 GAO report was for the NRC to improve its pre-licensing activities. As a result, the NRC ceased relying on the presumption that applicants for a license were acting in "good faith," and instead instituted a policy by which the NRC and the Agreement States would verify the legitimacy of applicants when first dealing with them. We also issued pre-licensing guidance that includes various applicant and licensee screening activities and site visits to ensure radioactive source will be used as intended.

Integrated Materials Performance Evaluation Program

In the area of materials security, the NRC and Agreement State regulatory agencies have worked together to create a strong and effective regulatory framework that provides an

appropriate level of security for risk-significant radioactive sources to ensure adequate protection of public health and safety, and provide for the common defense and security.

The Atomic Energy Act (AEA) gives the NRC preemptive authority over health and safety and common defense and security regulation of the possession and use of AEA materials. Subsequent amendments to the AEA added Section 274 of the Act which created the Agreement State program, under which the NRC may relinquish its health and safety authority of AEA material specified in formal agreements. When a State applies to become an Agreement State, the NRC reviews the State's regulatory program to ensure that the program is both adequate to protect public health and safety and compatible in all other respects with the NRC's own program. In addition, the AEA does not allow the NRC to relinquish the authority to protect the common defense and security to an Agreement State. Thus, the Commission retains the authority to impose security requirement on Agreement State licensees.

The AEA also requires the NRC to periodically review the 37 Agreement State programs. In 1997, the Commission fully implemented a process, the Integrated Materials Performance Evaluation Program (IMPEP), to assess its own regional materials programs as well as those of the Agreement States. The program uses a set of common performance indicators as a basis for an integrated assessment of a regional or Agreement State program. The IMPEP provides the NRC with a systematic, integrated, and reliable evaluation of the strengths and weaknesses of the respective programs. This in-depth process provides an indication of areas in which NRC and the Agreement States should dedicate more resources or management attention.

NRC Regulations (10 CFR Part 37)

Developing a radioactive source security rulemaking to replace the Orders and State requirements described above, and provide generally applicable requirements to a broad set of licensees required a significant collaborative effort between the NRC and the Agreement States. This rulemaking was informed by numerous insights regarding implementation of the Orders, as informed by inspections, self-assessments, and external audits. The challenge was to create a materials security rule that incorporated realistic approaches to enhancing security and that would interface and integrate well with the NRC's existing safety rules.

The resulting rule (10 CFR Part 37) is an optimized mix of performance-based and prescriptive requirements that provide the framework for a licensee to develop a security

program for risk significant materials with measures specifically tailored to their facilities. The rule became effective May 20, 2013; compliance was required for NRC licensees by March 19, 2014. Agreement State licensees must fulfill compatible requirements by March 2016. Key requirements include:

- Background checks, including fingerprinting, to help ensure that individuals with unescorted access to radioactive sources are trustworthy and reliable;
- Controlling personnel access to areas where risk-significant radioactive sources are stored and used;
- Documented security programs that are designed with defense in depth to detect, assess, and respond to actual or attempted unauthorized access events;
- Coordination and response planning between licensees and local law enforcement agencies for their jurisdiction;
- Coordination and tracking of radioactive source shipments; and
- Security barriers to discourage theft of portable devices that contain risk-significant radioactive sources.

Inspection and Enforcement

Trained NRC inspectors and investigators identify violations of security requirements through routine and special inspections. When violations of security requirements are identified, licensees are required to implement corrective actions before the inspector completes the inspection. NRC inspectors verify and evaluate these corrective actions during subsequent inspections. After a violation is identified, the NRC assesses the significance of a violation by considering the actual safety and/or security consequences, the potential consequences, and any willful aspects of the violation. Depending on the severity of the violation, the NRC may impose civil enforcement actions, and the licensee may also be subject to criminal prosecution.

The NRC has an extensive training program for personnel conducting security inspections. The NRC training program is available to Agreement States as well, and only qualified inspectors can conduct security inspections. Qualification requires a candidate both to complete training and to accompany qualified inspectors on inspections. In addition to providing training, the NRC also maintains a secure online information-sharing tool for NRC and Agreement State inspectors. This resource is available for inspectors seeking additional guidance to resolve questions related to security of risk-significant radioactive material.

GAO Audits

The NRC radioactive source security program has been the focus of two recent GAO audits. In the first audit, the GAO reviewed the NRC's security requirements for risk-significant radioactive sources possessed, and in use at U.S. medical facilities. However, because the 10 CFR Part 37 regulations were not in effect at the time of this most recent GAO audit, the GAO report focused on the NRC security requirements that were issued to licensees by Orders. As noted earlier, the Part 37 rule did not simply codify the security orders, but expanded upon the security requirements in those Orders. The 2012 GAO report concluded that the NRC security controls needed to be strengthened because they do not prescribe specific security measures (such as specific requirements on the use of cameras, alarms and other physical security measures) that the licensee should take to secure their radiation sources.

The NRC did not agree with this conclusion. The NRC believes prescriptive "one-size-fits-all" regulations may result in either excessive or non-conservative approaches to source security. The GAO based its conclusions on four examples identified during its field work to support their final report (out of 26 facilities GAO visited). The NRC and Agreement States conducted follow-up evaluations with three of the licensees GAO identified, and concluded that there was no violation of NRC security requirements. The NRC was unable to identify the fourth licensee to pursue further action. The NRC's and Agreement States' view is that such a failure to properly implement security controls would be a compliance issue to be addressed through inspection and enforcement. This example does not indicate that the performance based regulatory framework itself is inadequate.

While the NRC did not agree with the GAO recommendation for prescriptive-based regulation, the NRC did acknowledge the GAO concerns that some of the licensee personnel with security responsibility lack expertise in physical security, which may result in inconsistent application of security controls to their programs. In response to this recommendation, the NRC developed and provided additional written guidance to instruct licensees on best security practices. This best practices document is in addition to the implementation guidance document already developed to accompany the publication of 10 CFR Part 37.

The latest GAO audit reviewed the NRC program of security requirements for risk-significant radioactive sources used in industrial settings. In this audit, GAO raised concerns with how the NRC defines collocation of sources, the trustworthiness and reliability process (questioning whether it provides reasonable assurance against an insider threat), and the

development of the best security practices document (specifically that licensees were not directly involved in the development of this document).

Again, this GAO report focused on the NRC security requirements that were issued to licenses by Orders because the 10 CFR Part 37 regulations were not in effect at the time of the audit. The NRC acknowledges the concerns raised by the GAO in the most recent audit, and is committed to reviewing the effectiveness of the requirements to determine whether any additional security enhancements are necessary. If additional measures are needed, the Commission will consider appropriate security enhancements.

Federal Collaboration

Nuclear and radioactive materials are a critical and beneficial component of global medical, industrial, and academic efforts. Domestically, the NRC and the Department of Energy/National Nuclear Security Administration (NNSA) have worked together with a common goal of ensuring radioactive sources are not being used for malevolent purposes.

NNSA, through its Global Threat Reduction Initiative (GTRI), provides government-funded physical security enhancements to licensees on a voluntary basis. These voluntary enhancements are supplementary to, but do not replace, licensees' obligations to meet NRC and Agreement State regulatory requirements. The voluntary security enhancements go beyond the NRC's regulatory requirements. The NNSA program also provides other important and valuable benefits and enhancements, including removal of disused radioactive sources and specialized training for local law enforcement.

Looking Forward

Since September 11, 2001, the NRC and Agreement States have worked together to create a strong, effective regulatory framework that provides an appropriate level of security for risk-significant radioactive sources to ensure adequate protection of public health and safety, and the common defense and security. The NRC's efforts in radioactive source security have not ended with the publication and implementation of our 10 CFR Part 37 rule. The NRC will continue to assess its programs to ensure they promote the safe and secure use and management of radioactive sources.

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.