Congressional Research Service

"Dirty Bombs": Background in Brief

Jonathan Medalia
Specialist in Nuclear Weapons Policy

June 24, 2011

Congressional Research Service
7-5700
www.crs.gov
R41891

Summary

Congress has long sought, through legislation and oversight, to protect the United States against terrorist threats, especially from chemical, biological, radiological, and nuclear (CBRN) weapons. Radiological dispersal devices (RDDs) are one type of CBRN weapon. Explosive-driven "dirty bombs" are an often-discussed type of RDD, though radioactive material can also be dispersed in other ways. This report provides background for understanding the RDD threat and responses, and presents issues for Congress.

Radioactive material is the necessary ingredient for an RDD. This material is composed of atoms that decay, emitting radiation. Some types and amounts of radiation are harmful to human health.

Terrorists have shown some interest in RDDs. They could use these weapons in an attempt to cause panic, area denial, and economic dislocation. While RDDs would be far less harmful than nuclear weapons, they are much simpler to build and the needed materials are used worldwide. Accordingly, some believe terrorists would be more likely to use RDDs than nuclear weapons. Key points include:

- RDDs could contaminate areas with radioactive material, increasing long-term cancer risks, but would probably kill few people promptly. Nuclear weapons could destroy much of a city, kill tens of thousands of people, and contaminate much larger areas with fallout.
- Cleanup cost after an RDD attack could range from less than a billion dollars to tens of billions of dollars, depending on area contaminated, decontamination technologies used, and level of cleanup required.
- Terrorists would face obstacles to using RDDs, such as obtaining materials, designing an effective weapon, and avoiding detection.

Governments and organizations have taken steps to prevent an RDD attack. Domestically, the Nuclear Regulatory Commission has issued regulations to secure radioactive sources. The Department of Homeland Security develops and operates equipment to detect radioactive material. The National Nuclear Security Administration has recovered thousands of disused or abandoned sources. Some state and local governments have taken steps to prepare for an RDD attack. Internationally, the International Atomic Energy Agency has led efforts to secure radioactive sources. Its Code of Conduct on the Safety and Security of Radioactive Sources offers guidance for protecting sources. The G8 Global Partnership has secured sources in Russia and elsewhere. Other nations have taken steps to secure sources as well. Key points include:

- Nuclear Regulatory Commission actions have done much to instill a security culture for U.S. licensees of radioactive sources post-9/11.
- Many programs have sought to improve the security of radioactive sources overseas, but some incidents raise questions about security.

Should prevention fail, federal, state, and local governments have taken many measures to respond to and recover from an RDD attack. The National Response Framework "establishes a comprehensive, national, all-hazards approach to domestic incident response." The federal government has expertise and equipment to use for recovery. Key points include:

- Government agencies have done much to prepare for and recover from an RDD attack. This work would help cope with other disasters. Conversely, planning for other disasters would help in the event of an RDD attack.
- Response planning fell short in the wake of Katrina and the Gulf oil spill, raising questions about the effectiveness of planning to respond to an RDD attack.

Issues for Congress include:

- The priority for countering RDDs vs. other types of CBRN weapons.
- The proper balance of effort for securing domestic vs. overseas radioactive sources.
- Whether to establish a radiation detection system in cities; how to dispose of potentially large volumes of radioactive waste that could result from an RDD attack.
- Whether to modify the pace of a program for implementing certain security enhancements for U.S. radioactive sources.
- How to improve radiological forensics capability.

This report is an abridged version of CRS Report R41890, *"Dirty Bombs": Technical Background, Attack Prevention and Response, Issues for Congress,* by Jonathan Medalia.

Contents

Figures

Contacts

Radiation and Its Effects

Radioactive materials are used worldwide for medical, industrial, research, and other purposes. Yet their security is far from airtight, especially in foreign countries. Terrorists could create a radiological dispersal device (RDD) by obtaining radioactive material and detonating an explosive next to it. An attack could contaminate some square miles, disrupt the economy, cost tens of billions of dollars to remediate, increase the long-term cancer rate, and cause panic in the target area and beyond. While the press focuses on explosive-driven "dirty bombs," terrorists could also disperse radioactive material from aircraft or in other ways. This report examines radiation and its effects, steps to prevent, respond to, and recover from an attack, and issues for Congress.

Many atoms are stable: they remain in their current form indefinitely. Some are unstable, or radioactive. They "decay," often by emitting energetic particles.[1] Gamma rays, a form of electromagnetic radiation, are often emitted by decay. Each radioactive atom, or "radionuclide," decays in a specific way. Some high-energy radiation is "ionizing." Most atoms have no net electrical charge because they have an equal number of positively-charged protons and negatively-charged electrons. Ionizing radiation knocks electrons off atoms, turning atoms into positively-charged ions that damage living cells. Very low doses of radiation produce few if any effects, but progressively higher doses may increase the risk of cancer or may cause radiation sickness or death. In the United States, dose is usually measured in units of rem. This unit takes into account the amount of radiation absorbed and its biological effects. The average background dose for the U.S. population is estimated at 620 millirem (mrem; 1,000 mrem = 1 rem) per year.[2] About half is from natural sources, and half from exposure for medical purposes.

An RDD attack is likely to expose few people to a dose of more than a few rem per year. Views differ on the harm from that dose. One view is that any amount of radiation increases cancer risk; another is that there is no evidence that radiation of less than about 10 rem per year increases that risk. Federal standards differ for low doses. For dose to the public resulting from the nuclear fuel cycle (e.g., nuclear power plants), the Environmental Protection Agency (EPA) uses a standard of 25 mrem per year of whole-body dose.[3] In contrast, the Nuclear Regulatory Commission (NRC) has established an occupational dose limit of 5 rem per year.[4] No single level marks the line between an acceptable and unacceptable dose.

An RDD attack would elevate dose in the affected area beyond the background dose. The EPA issued guidance for protective actions following nuclear and radiological incidents except nuclear war, and the Federal Emergency Management Agency (FEMA) issued guidance for actions following RDD and improvised nuclear device (IND, i.e., a terrorist-made nuclear weapon) incidents.[5] Both agencies recommended "protective action guides" (PAGs). A PAG is "the

---

[1] The most common types of particles emitted in decay are alpha particles (two protons plus two neutrons), beta particles (an electron or positron, with the latter being a positively-charged electron), and, for heavy elements, neutrons.

[2] National Council on Radiation Protection and Measurement, *Ionizing Radiation Exposure of the Population of the United States*, report 160 (2009), available via http://www.ncrppublications.org/Reports/160. The figure of 620 mrem is from "NCRP Report No. 160 Section 1 Pie Chart," http://www.ncrponline.org/Publications/160_Pie_charts-Sec1.html.

[3] 10 CFR 190.10(a).

[4] 20 CFR 1201(a)(1)(i).

[5] U.S. Environmental Protection Agency. Office of Radiation Programs. *Manual of Protective Action Guides and* (continued...)

projected dose to a reference individual, from an accidental or deliberate release of radioactive material, at which a specific protective action to reduce or avoid that dose is recommended."[6]

FEMA divides incident response into phases. For the early phase, which starts "at the beginning of the incident,"[7] the protective action recommended for a PAG of 1 to 5 rem is sheltering in place or evacuation. The intermediate phase "is usually assumed to begin after the incident source and releases have been brought under control." For it, FEMA recommends "relocation of the public" for a projected dose of 2 rem for the first year and 0.5 rem per year for any subsequent year. The late phase starts when recovery and cleanup begin, and ends with their completion. FEMA does not have a PAG for the late phase because authorities would need to optimize among economic, land use, etc., in determining which areas need to be remediated to what levels.

As a guide to quantities of material that should be protected, in 2003 the International Atomic Energy Agency (IAEA) revised its Code of Conduct on the Safety and Security of Radioactive Sources.[8] The IAEA decided that the code "should serve as guidance to States for—*inter alia*—the development and harmonization of policies, laws and regulations on the safety and security of radioactive sources."[9] It lists 16 radionuclides that are in common use and could pose a threat. For each radionuclide, the code lists three categories of radiation and the threshold radiation value for each category based on potential to harm individuals. Category 1 sources are those that, if not safely managed or securely protected, could cause permanent injury to someone who handled them for a few minutes, and death to someone who handled them unshielded for a few minutes to an hour. For Category 2 sources, the corresponding figures are minutes to hours and hours to days. Category 3 sources could cause injury to someone handling them for some hours.[10] Of the 16 radionuclides, cesium-137 chloride is of particular concern.[11] Category 2 quantities are often a fraction of a gram. Somewhat larger amounts can contaminate a substantial area. For example, **Figure 1** models a possible RDD attack on Washington, DC, using about 50 grams of cesium-137 chloride, which contaminates, to different levels, 0.81 to 5.10 square miles. The Energy Policy Act of 2005 (P.L. 109-58) mandates certain security measures for Category 1 and 2 sources. The NRC considers Category 2 sources to be risk-significant.[12] Since the NRC judges that Category 2 sources could cause significant economic effects, it uses Category 2 as the basis for mandating security measures beyond those in the Energy Policy Act.

Threats and Impediments

An RDD could cause prompt casualties, which would most likely come only from the explosion of a dirty bomb; panic; economic disruption, which might result if a port or city center were

(...continued)

Protective Actions for Nuclear Incidents, revised 1991; and Federal Emergency Management Agency, "Planning Guidance for Protection and Recovery Following Radiological Dispersal Device (RDD) and Improvised Nuclear Device (IND) Incidents," 73 *Federal Register* 45029-45048, August 1, 2008.

6 Ibid., p. 45034.

7 Quotes in this paragraph are from ibid., pp. 45032 and 45035.

8 International Atomic Energy Agency, *Code of Conduct on the Safety and Security of Radioactive Sources*, January 2004, http://www.iaea.org/Publications/Booklets/RadioactiveSources/radioactivesource.pdf.

9 Ibid., p. 2.

10 Ibid., p. 15.

11 National Research Council. *Radiation Source Use and Replacement, Abbreviated Version*, p. 7.

12 Nuclear Regulatory Commission, "Physical Protection of Byproduct Material: Proposed Rule," 75 *Federal Register* 33902, June 15, 2010.

contaminated with radioactive material; asset denial, in which public concern over the presence of radioactive material might lead people to abandon a subway system or an area of a city for months to years; a requirement for decontamination, which would be costly; and long-term casualties resulting from exposure to or inhalation of radioactive material. A study of the economic impacts of an attack on the ports of Los Angeles and Long Beach using two RDDs placed total U.S. losses at $8.5 billion for exports and $26.0 billion for imports.[13]

While there have been thefts of radioactive material and attempts to use it for malevolent ends,[14] there has not been a successful RDD attack, for reasons such as the following. Terrorists would need to learn about radiation for self-protection. They would need to learn which radioactive materials would be suitable for an RDD. They would have to obtain the material despite security measures. They would have to move the material past detectors at U.S. ports and elsewhere. They would have to acquire the other bomb components, assemble the bomb, and place it, steps that law enforcement might detect. Forensic analysis might reveal the perpetrator of the attack, possibly leading to retaliation and deterring state assistance. While no one reason presents an insurmountable obstacle, the combination may help explain why an RDD attack has not occurred.

Preventing an Attack: Domestic Efforts

Before September 11, 2001, the main concern for radioactive sources was their safe handling. They were used worldwide in many applications with varying levels of security. The ongoing U.S. response to the attacks is based on "layered defense," in which each layer increases the likelihood of disrupting a possible attack. Layers includes protecting sources through licensing, tracking, and physical security upgrades; removing sources that are outside the tracking system because they are abandoned, lost, or stolen; and reducing the number of sources in use.

Securing Radioactive Sources

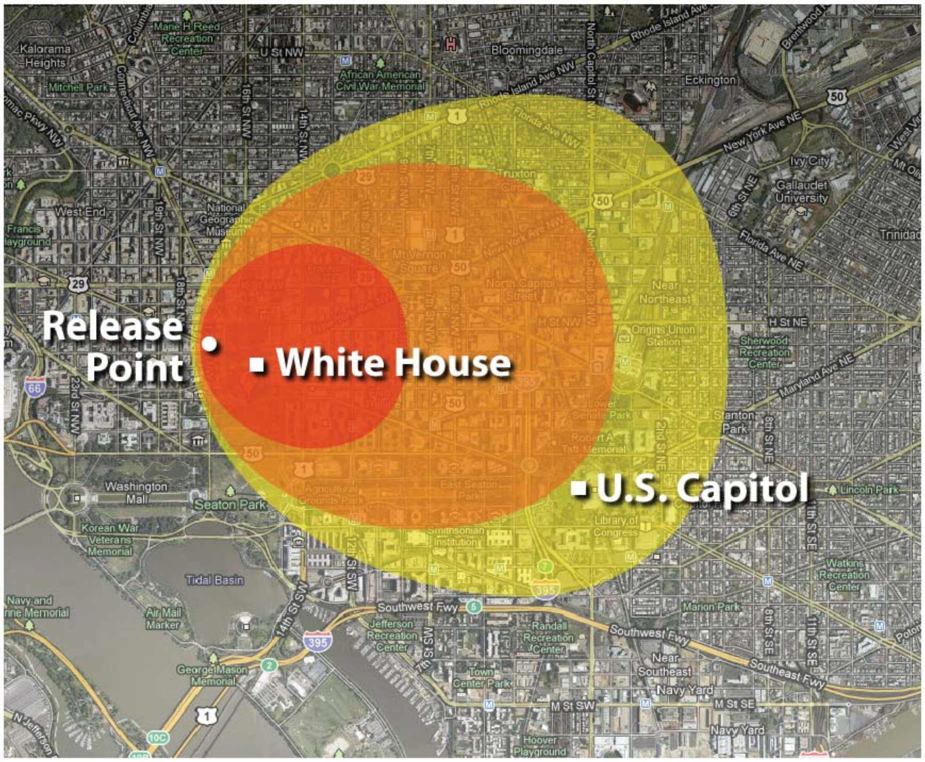
Since materials of greatest concern for use in an RDD are made in nuclear reactors, terrorists could only obtain them through transfer from sympathetic insiders, theft, or purchase. Securing radioactive sources therefore reduces the risk of an RDD attack. Many government agencies and other entities have taken steps to secure these sources.

The Nuclear Regulatory Commission (NRC), an independent agency, "has the responsibility to license and regulate the civilian use of radioactive materials for commercial, industrial, academic, and medical purposes in a manner that protects public health and safety and promotes the common defense and security. The NRC and its predecessor, the Atomic Energy Commission (AEC), have regulated the use of radioactive materials since 1946."[15] Since 9/11, the NRC has issued orders and regulations requiring its licensees to take various measures to enhance radiation source security.

[13] JiYoung Park, "The Economic Impacts of Dirty Bomb Attacks on the Los Angeles and Long Beach Ports: Applying the Supply-Driven NIEMO (National Interstate Economic Model," *Journal of Homeland Security and Emergency Management,* vol. 5, no. 1 (2008), article 21, p. 10, http://www.bepress.com/jhsem/vol5/iss1/21/.
[14] See Nuclear Threat Initiative, *Radiological Terrorism Tutorial,* "History of Radiological Incidents."
[15] U.S. Nuclear Regulatory Commission. "Request for Comments on the Draft Policy Statement on the Protection of Cesium-137 Chloride Sources and Notice of Public Meeting," NRC-2010-0209, *Federal Register*, vol. 75, no. 124, June 29, 2010, p. 37484.

Figure 1. A Possible RDD Attack on Washington, DC

Using about 50 Grams of Cesium-137 Chloride



Effects and Actions							
	Area km²	Area mi	Equivalent Dose (rem)	Exceeds relocation PAG for which year:	Population	All Cancers	Fatal Cancers
(red)	2.10	0.81	>2.00	First year only	38,000	233	159
(orange)	7.60	2.93	>0.500	Any subsequent year	94,700	278	189
(yellow)	13.2	5.10	>5.00	50 years (cumulative)	125,000	461	314
Areas and counts are cumulative. RDD detonated at 38.9 N, 77.0 W. PAG: Protective Action Guide							

Source: William Rhodes III, Senior Manager, International Security Systems Group, Sandia National Laboratories, September 2010; analysis by Heather Pennington; graphics by Mona Aragon.

Notes: (provided by William Rhodes): This map, based on an atmospheric dispersion model, shows where individuals are projected to have an increased risk of developing cancers due to radiation exposure over a year or more. The RDD in this scenario uses about 50 grams of cesium-137 chloride. The model assumes that all material used is dispersed, but that it is not dispersed evenly over the area. Wind is assumed to be from west to east at 7 mph. The model includes exposure from radioactive material both deposited on the surface and resuspended into the air and inhaled. EPA and FEMA have developed Protective Action Guides (PAGs) to indicate when long-term relocation of individuals should be considered. PAGs are primarily based on an assessment of the increased risk of developing cancer over an exposed individual's lifetime. They assume, conservatively, that individuals are unsheltered and remain in the area during the entire period described for each contour. Contours show where individuals, if not relocated per the PAG, are projected to receive at least a specified dose in a specified time, as follows: inner contour (red), dose in first year post-attack, >2.00 rem; middle contour (orange), dose in second year post-attack, >0.500 rem; and outer contour (yellow), cumulative dose in the first 50 years post-attack. >5.00 rem. The cigar-shaped plumes often seen in models of atmospheric dispersion occur for gases or very fine particles, which would be the case for chemical warfare agents or fallout from a nuclear weapon but not in the case depicted. Whether such plumes would occur for an RDD depends on such factors as wind speed, type of explosive, and particle size.

The National Nuclear Security Administration (NNSA) is a semiautonomous agency within the Department of Energy. The Global Threat Reduction Initiative (GTRI) is a key NNSA program to enhance the security of radioactive sources. GTRI's Domestic Materials Protection Program enhances security for domestic radioactive sources on a voluntary basis, and pays for upgrades and initial maintenance. GTRI's Off-site Source Recovery Project recovers sources in the United States and abroad that have been lost, abandoned, or stolen, or are excess to a user's needs. As of March 28, 2011, OSRP had recovered 24,029 sources in the United States.[16]

The Energy Policy Act of 2005 established the **Radiation Source Protection and Security Task Force** with a mandate to "evaluate, and provide recommendations relating to, the security of radiation sources in the United States from potential terrorist threats." Its members represent many federal agencies. Its 2010 report[17] identified two major challenges, access to disposal pathways for unused sources, and alternatives to several risk-significant radioactive sources.

The Environmental Protection Agency (EPA) "is seeking to reduce the number of sealed radiation sources used in industrial devices and applications. Through its Alternative Technologies Initiative, the Agency has been working with industry since 2001 to identify non-nuclear substitutes."[18] The Domestic Nuclear Detection Office, a component of the Department of Homeland Security (DHS), is supporting similar R&D through its Small Business Innovative Research program. The Department of Defense (DOD) has some sealed sources in the United States, such as at hospitals. The NRC grants DOD components one or more licenses, and they protect the sources in accordance with NRC regulations.[19]

How Secure Are Radioactive Sources in the United States?

NRC notes such security violations as "inoperable or ineffective physical protection systems" and "incomplete or inadequate plan with local law enforcement."[20] The Radiation Source Protection and Security Task Force stated, "Every year, thousands of sources become disused and unwanted in the United States. … the longer sources remain disused or unwanted the chances increase that they will become unsecured or abandoned."[21] (Most of these sources have a very low level of radioactivity and do not pose a significant risk.[22]) Nonetheless, there have been "no successful thefts or sabotage" of higher-level sources,[23] and there has never been a successful RDD attack. NRC data show that from the third quarter of FY2006 through the second quarter of FY2010, no Category 1 or 2 sources were lost, and 17 Category 3 sources were lost but all were recovered.[24]

[16] Los Alamos National Laboratory, "OSRP Sources Recovered," as of March 28, 2011, http://osrp.lanl.gov/images/Maps/Recoveries_to_Date.pdf.

[17] U.S. Radiation Source Protection and Security Task Force. *The 2010 Radiation Source Protection and Security Task Force Report,* August 2010, http://www.nrc.gov/security/byproduct/2010-task-force-report.pdf.

[18] U.S. Environmental Protection Agency. "Alternative Technologies for Industrial Applications," http://www.epa.gov/radiation/source-reduction-management/alt-technologies.html.

[19] Information provided by Chemical, Biological, Radiological, and Nuclear Directorate, Office of Homeland Defense Integration and Defense Support of Civil Authorities, Office of the Secretary of Defense, Department of Defense, personal communication, September 15, 2010, and by Nuclear Regulatory Commission, February 10, 2011.

[20] U.S. Nuclear Regulatory Commission. "Security Inspections and Enforcement," briefing slides 5-8, no date. NRC provided these slides to CRS July 31, 2010.

[21] U.S. Radiation Source Protection and Security Task Force. *The 2010 … Report,* p. 31.

[22] Personal communication, Nuclear Regulatory Commission, November 30, 2010.

[23] U.S. Nuclear Regulatory Commission. "Security Inspections and Enforcement," slide 19.

[24] Idaho National Laboratory, "Nuclear Material Events Database: Quarterly Report, Second Quarter Fiscal Year 2010," by Thomas Smith and Robert Sant, INL/EXT-10-18136 (FY 2010 Qtr 2), July 2010, p, 5.

Detecting Radioactive Sources

U.S. Customs and Border Protection, a DHS component, has deployed systems at ports and border crossings to detect and identify radioactive material (and other contraband) entering the United States. Other DHS components deploy radiation detection equipment at other sites inside the United States, and the Domestic Nuclear Detection Office has a cooperative program with state and local agencies to deploy such equipment. These systems seek to detect terrorist nuclear weapons or nuclear-weapon material while minimizing the impact on legitimate commerce, but could detect RDD-suitable material as well. CRS Report R40154, *Detection of Nuclear Weapons and Materials: Science, Technologies, Observations*, by Jonathan Medalia, discusses detection.

Intelligence and Counterterrorism

Many U.S. agencies contribute and analyze intelligence on potential CBRN terrorist threats. The 9/11 Commission noted shortcomings in the Intelligence Community.[25] In response, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA, P.L. 108-458). This act established the position of Director of National Intelligence, who is to "serve as head of the intelligence community." Section 6905, "Radiological Dispersal Devices," makes it unlawful to acquire or possess RDDs. IRTPA established the National Counterterrorism Center to analyze and integrate intelligence on terrorism, except that pertaining to domestic terrorists and domestic counterterrorism. IRTPA directed the President to establish the National Counter Proliferation Center to analyze proliferation-related intelligence. Within the United States, the Federal Bureau of Investigation is the lead agency for counterterrorism intelligence. It "created a Directorate of Intelligence in its headquarters to produce intelligence analysis."[26]

Preventing an Attack: Global Efforts

Securing Radioactive Sources

Because an RDD attack might occur outside the United States, or material obtained abroad might be used for an RDD attack on this nation, the United States and others—including international organizations and foreign governments—are working to secure sources worldwide.

International Organizations

International Atomic Energy Agency (IAEA)

The IAEA, a U.N. organization, has responsibilities in such areas as nuclear energy, peaceful applications of nuclear science and technology, nuclear nonproliferation, and nuclear safety and security. It has the lead international role in efforts to secure radioactive sources. For example, it

[25] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report,* New York, Norton, 2004, p. vii.

[26] "A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack," a special report by Joseph I. Lieberman, Chairman, and Susan M. Collins, Ranking Member, United States Senate Committee on Homeland Security and Governmental Affairs, February 3, 2011, p. 53.

issued a Code of Conduct on the Safety and Security of Radioactive Sources, as discussed earlier. Its 2010-2013 Nuclear Security Plan covers the global nuclear security framework, nuclear security services, and security improvement.[27] It helps countries remove orphan radioactive sources; provides training in Asia, Africa, and South America "for regaining control over sealed sources"; and trains customs authorities in radiation monitoring.[28] It maintains an International Catalogue of Sealed Radioactive Sources and Devices to help identify sealed sources so they can be handled safely.[29]

G8 Global Partnership

In June 2002, the G8 committed to "six principles to prevent terrorists or those that harbour them from acquiring or developing" CBRN weapons, established the G8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction to implement these principles, and committed to raise "up to $20 billion" over ten years for projects supporting the partnership.[30] The partnership has many programs to reduce CBRN threats.[31]

Global Initiative to Combat Nuclear Terrorism

This initiative was established in 2006 by 13 governments.[32] Its principles include "develop, if necessary, and improve accounting, control and physical protection systems for nuclear and other radioactive materials and substances," and "improve the ability to detect nuclear and other radioactive materials and substances in order to prevent illicit trafficking in such materials and substances, to include cooperation in the research and development of national detection capabilities that would be interoperable."

U.S. Programs

National Nuclear Security Administration

Some GTRI programs seek "to identify, secure, remove and/or facilitate the disposition of high risk vulnerable nuclear and radiological materials around the world, as quickly as possible, that pose a threat to the United States and the international community."[33] The Off-site Source Recovery Project has removed 985 sources from 15 other nations as of September 2010.[34] Another NNSA program, Second Line of Defense (SLD), "strengthens the capability of foreign

[27] International Atomic Energy Agency. Board of Governors. General Conference. "Nuclear Security Plan 2010-2013." GOV/2009/54-GC(53)/18, August 17, 2009, pp. 8-12.

[28] International Atomic Energy Agency, "Improving the Safety and Security of Sealed Radioactive Sources," accessed May 2, 2011, http://www.iaea.org/Publications/Booklets/SealedRadioactiveSources/activities.html.

[29] International Atomic Energy Agency, "International Catalogue of Sealed Radioactive Sources and Devices (ICSRS)," http://nucleus.iaea.org/CIR/CIR/ICSRS.html, updated 2010.

[30] G8, "The G8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction," June 27, 2002.

[31] G8, "Report on the G-8 Global Partnership 2010," last modified February 11, 2011.

[32] For links to key documents on the Global Initiative, see U.S. Department of State. "The Global Initiative To Combat Nuclear Terrorism," http://www.state.gov/t/isn/c18406.htm.

[33] U.S. Department of Energy. National Nuclear Security Administration. "GTRI: Reducing Nuclear Threats," January 2009, http://www.nnsa.energy.gov/news/2330.htm.

[34] Los Alamos National Laboratory, Off-site Source Recovery Program, "OSRP Operations Worldwide."

governments to deter, detect, and interdict illicit trafficking in nuclear and other radioactive materials across international borders and through the global maritime shipping system."[35]

Nuclear Regulatory Commission

The NRC helps regulators in other nations implement the IAEA Code of Conduct, such as by helping them develop national registries of radioactive sources, helping them with safety and security regulatory oversight, and holding workshops that describe the NRC's requirements for physical protection of materials and the U.S. regulatory framework.[36]

Department of State

The Export Control and Related Border Security (EXBS) program strengthens border security and control of strategic exports, thereby "bolster[ing] partner countries' capabilities to detect and interdict illicit transfers of strategic items, radioactive materials, and other WMD components" It assists 46 countries.[37] The Weapons of Mass Destruction Terrorism program conducts projects to counter a terrorist CBRN attack. The department supports the Global Initiative to Combat Nuclear Terrorism.

Department of Defense

The U.S. Strategic Command coordinates global U.S. counter-CBRN efforts.[38] The Defense Threat Reduction Agency is DOD's combat support agency in this effort.[39] The two agencies operate the U.S. Strategic Command Center for Combating Weapons of Mass Destruction, which "synchronizes Combating Weapons of Mass Destruction efforts across our military's geographic commands."[40]

Programs of Other Nations

Other nations have taken steps to control their own radioactive material and to help secure such material elsewhere. Canada, in cooperation with GTRI, provided funds for removing 59 Russian radioisotopic thermoelectric generators (RTGs), which contain large amounts of radioactive material and are typically deployed unattended in remote areas.[41] Pakistan's Nuclear Regulatory Authority is implementing a National Nuclear Security Action Plan in coordination with the IAEA that manages high-risk radioactive sources, provides detection equipment at key points, and

[35] Department of Energy, *FY 2011 Congressional Budget Request*. volume 1, p. 371.

[36] U.S. Nuclear Regulatory Commission and National Nuclear Security Administration, *Partnership for Securing Nuclear and Radiological Materials*, March 31, 2010, p. 2.

[37] U.S. Department of State., *Fiscal Year 2011 Congressional Budget Justification: Volume 2, Foreign Operations*, 2010, p. 176, http://www.state.gov/documents/organization/137936.pdf.

[38] U.S. Strategic Command. "USSTRATCOM Center for Combating Weapons of Mass Destruction (SCC-WMD)," February 2011.

[39] U.S. Department of Defense. Defense Threat Reduction Agency and USSTRATCOM Center for Combating WMD. "About DTRA/SCC-WMD," http://www.dtra.mil/About.aspx.

[40] Ibid.

[41] Canada. Department of Foreign Affairs and International Trade. Personal communication, May 24, 2011.

secures orphan sources.[42] Poland's state-owned Radioactive Waste Management Plant (RWMP) has been involved in the GTRI program for securing radioactive sources in Poland that has upgraded security in more than 70 institutions, including almost all oncology clinics and regional blood banks.[43] The Korean Institute for Nuclear Safety has developed a Radiation Safety Information System to trace radioactive sources through their life cycle, and a system to track misplaced or stolen industrial radiography sources in real time.[44]

How Secure Are Radioactive Sources in Other Nations?

Despite efforts to secure radioactive sources, vulnerabilities persist. The IAEA's Illicit Trafficking Database (ITDB) has data on the vulnerability of nuclear and other radioactive sources. According to the agency, "From 1 July 2009 to 30 June 2010, States reported 222 incidents to the ITDB; 120 of these were reported to have occurred during this period and the remaining 102 were reports of prior incidents. Twenty-one of the incidents reported involved such activities as unauthorized possession and/or attempts to sell or smuggle nuclear material or radioactive sources. …One-hundred and forty reported incidents involved unauthorized activities without apparent relation to criminal activity."[45] According to the U.S. Department of State, "Of the 222 events reported to the IAEA from 1 July 2009 to 30 June 2010 involving radiological and nuclear materials outside legitimate control, most involved incidents overseas and roughly 10 percent occurred in the U.S. All of the incidents the U.S. reported to the IAEA during this time involved detections of radioactively contaminated materials coming into the U.S."[46]

In 2009, the IAEA reported "a persistent problem with illicit trafficking in nuclear and other radioactive materials, with thefts, losses and other unauthorized activities and events." Of the 1,562 confirmed incidents in the ITDB for 1995-2008, 421 involved reports of theft or loss, which IAEA called "indicative of vulnerabilities in security and control systems." Another 336 involved unauthorized possession or related criminal activities, with the number possibly higher. The 724 incidents of other unauthorized activities and events "have mainly involved radioactive sources, including some … high-risk 'dangerous' sources, and radioactively contaminated materials. Occurrence of such incidents is an indication of failures in systems to control, secure and dispose of radioactive materials. They also show weaknesses of regulatory systems." [47]

[42] Embassy of Pakistan, Washington, DC, personal communication, May 17, 2011.

[43] Information provided to CRS by the National Atomic Energy Agency, Warsaw, Poland, May 16, 2011.

[44] Republic of Korea, Korea Institute of Nuclear Safety, "Country Report on (RAS/9/042), 'Sustainability of Regional Radiation Protection Infrastructure,'" 2009, p. 22.

[45] International Atomic Energy Agency, Board of Governors, *Nuclear Security Report 2010: Measures to Protect Against Nuclear Terrorism*, Report by the Director General, GOV/2010/42-GC(54)/9, August 12, 2010, p. 4.

[46] Personal communication, Department of State, May 6, 2011.

[47] Material on ITDB in this paragraph is from International Atomic Energy Agency, "IAEA Illicit Trafficking Database (ITDB)," September 2009, pp. 1-5, http://www-ns.iaea.org/downloads/security/itdb-fact-sheet-2009.pdf.

Attack Response, Recovery, and Attribution

Organization and Planning for Response

If an RDD attack occurred, effective response could save lives and speed recovery. Accordingly, the federal government has planned for a response. Key authorities for response include the Stafford Act, P.L. 100-707, which authorizes the President to declare an event a disaster, thereby allowing federal agencies to assist state and local governments, the Homeland Security Act of 2002, P.L. 107-295, which establishes the Department of Homeland Security; Homeland Security Presidential Directive 5, "Management of Domestic Incidents," 2003, which makes the Secretary of Homeland Security "the principal Federal official for domestic incident management"; and the National Response Framework (NRF), which "presents the guiding principles that enable all response partners to prepare for and provide a unified national response to disasters and emergencies—from the smallest incident to the largest catastrophe."[48]

The NRF has various annexes. The Nuclear/Radiological Incident Annex "describes the policies, situations, concepts of operations, and responsibilities of the Federal departments and agencies governing the immediate response and short-term recovery activities for incidents involving release of radioactive materials."[49] It spells out which agency would have the lead or would provide support in various incidents, and the capabilities and responsibilities of each. According to the Framework, DHS would be the lead agency for "all deliberate attacks involving nuclear/radiological facilities or materials, including RDDs or INDs."[50] In 2008, FEMA issued its "Planning Guidance for Protection and Recovery Following Radiological Dispersal Device (RDD) and Improvised Nuclear Device (IND) Incidents," which provides detailed guidance on response.[51] Some states and localities have developed response plans and held exercises.

An issue for any disaster plan is how well it would work in practice. An assessment of state radiation emergency preparedness found, "in almost every measure of public health capacity and capability, the public health system remains poorly prepared to adequately respond to a major radiation emergency incident."[52] A 2011 press report raised similar concerns about national preparedness.[53] Governments have planned responses to hurricanes, yet the overall response to Hurricane Katrina was poor. The Deepwater Horizon disaster occurred despite the federal government's National Oil and Hazardous Substances Pollution Contingency Plan.

48 For further information on the National Response Framework, see U.S. Department of Homeland Security. Federal Emergency Management Agency. "NRF Resource Center," http://www.fema.gov/emergency/nrf/.

49 U.S. Department of Homeland Security. Federal Emergency Management Agency. "Nuclear/Radiological Incident Annex," June 2008, p. NUC-1, http://www.fema.gov/pdf/emergency/nrf/nrf_nuclearradiologicalincidentannex.pdf.

50 Ibid., p. NUC-9.

51 U.S. Department of Homeland Security. Federal Emergency Management Agency. "Planning Guidance for Protection and Recovery Following Radiological Dispersal Device (RDD) and Improvised Nuclear Device (IND) Incidents," notice of final guidance, *Federal Register,* vol. 73, no. 149, August 1, 2008. pp. 45029-45048.

52 Council of State and Territorial Epidemiologists, "The Status of State-Level Radiation Emergency Preparedness and Response Capabilities, 2010," October 6, 2010, p. 13, http://www.cste.org/webpdfs/2010raditionreport.pdf.

53 Sheri Fink, "U.S. Health-Care Systems Said to Be Unprepared for Nuclear Disaster" *Washington Post,* March 8, 2011, p. 3.

Response and Recovery

As noted earlier, FEMA divides response into early, intermediate, and late phases. The source of resources would shift with the phase. In the early phase, state and local first responders would be the primary ones available. They would focus on minimizing deaths and injuries from radiation and panic. The intermediate phase would involve higher-level care for those suffering from radiation injuries, longer-term relocation of people from areas with dangerous levels of radioactivity, and initial stages of recovery, such as decontamination. Many federal resources could be brought to bear in this phase. Late-phase efforts would focus on recovery. The main activity would be reduction of radiation hazards to an acceptable level, such as by decontaminating streets and buildings, demolishing and replacing buildings that could not be cost-effectively decontaminated, or declaring certain areas off-limits. The federal government would presumably supply the specialized expertise, techniques, equipment, and supplies required.

In 2009, President Obama directed the establishment of the White House Long-Term Disaster Recovery Working Group. It is preparing a framework document with a strategy for dealing with recovery from all disasters and a report on long-term recovery from major disasters. As of June 2011, the former is in interagency review, and the latter is in the process of gaining concurrence among the organizations drafting it. No date had been set for release of either document.[54]

Researchers have studied various decontamination methods. One study found that for radioactive materials like cesium that bond with concrete and tile, washing with water would have little effect,[55] but that a solution of water with ammonium oxalate or ammonium chloride is more effective.[56] Idaho National Laboratory is investigating the use of lasers for decontamination.[57] Argonne National Laboratory is developing a "supergel" intended "to safely capture and dispose of radioactive elements in porous structures outdoors, such as buildings and monuments, using a spray-on, super-absorbent gel and engineered nanoparticles," for use in the event of an RDD attack.[58] EPA's National Homeland Security Research Center conducts decontamination research.[59]

Attribution

If an attack occurred, the United States would surely want to retaliate against the perpetrators. Retaliation would require attribution, i.e., identifying the attacker and the source of material. Attribution relies on forensics, i.e., a fusion of evidence gathered from intelligence, law enforcement, and scientific analysis of material from the weapon. *Nuclear* forensics has been conducted for many decades. It matches samples of pre- or post-detonation weapon material to an archive of samples from facilities producing such material, or against a library of information from manufacturers. (Government agencies use "archive" to refer to a collection of physical samples and "library" to refer to a collection of information.) It looks for clues that link to other

[54] Personal communication, Federal Emergency Management Agency, June 14, 2011.

[55] J. Real et al., "Mechanisms of Desorption of 134Cs [cesium-134] and 85Sr [strontium-85] Aerosols Deposited on Urban Surfaces," *Journal of Environmental Radioactivity,* 62 (2002), p. 1.

[56] Ibid., p. 1.

[57] Mike Wall, "INL Laser Research Could Help U.S. Respond to Terror Attack," April 19, 2010.

[58] Argonne National Laboratory. "'Supergel' System for Cleaning Radioactively Contaminated Structures."

[59] U.S. Environmental Protection Agency. Homeland Security Research. http://www.epa.gov/nhsrc/. The center's reports on RDDs are available at http://tinyurl.com/3kfyntf.

types of evidence, such as records of missing material. It identifies manufacturing processes, and may use simulation to see if a certain process could have led to a certain sample. By providing data on weapon materials and design, forensics could help determine the technical sophistication of the group that launched a nuclear attack, and which nations provided technical support, materials, or a weapon. To support this effort, the United States is developing a consolidated library and archive of nuclear material:[60] The potential to identify the source of material and the perpetrator of an attack supports deterrence and, if deterrence failed, could support retaliation.

Radiological forensics uses many of these techniques. It might be able to determine the age of a sample, perhaps eliminating some manufacturers as its source. Also, as DHS states, "non-rad[ioactive] evidence associated with the RDD will play an important role in the technical forensics investigation." Further, "Additional useful insights can be garnered from license information, sales records, vendor catalogs, etc., and this information is being collected as funding and accessibility allow."[61] The NRC and IAEA have libraries of information on sealed radioactive sources [62] that, according to one report, were not intended for forensics.[63] Since most sealed sources are made in foreign countries, DHS is funding Argonne and Idaho National Laboratories to gather data on these sources for forensics purposes.[64] Based on communications in 2011 between CRS and knowledgeable individuals at various government agencies and laboratories, there does not appear to be an archive of radioactive sources or materials.

Radiological and nuclear forensics differ in various ways. A nuclear explosion produces hundreds of radionuclides; materials that might be used in an RDD, excepting spent fuel, would likely have one or a few radionuclides, providing fewer clues. RDD radionuclides have half-lives measured in years, not hours or less, so collecting samples would not be as time-urgent as for a nuclear explosion. Nuclear forensics could support retaliation, depending on the country of origin of the material. In contrast, RDD material might be produced in one country, distributed by a second, sold to a third, and perhaps resold to a fourth, where terrorists might steal it. Argentina, Canada, several European countries, and Russia are the main producers of key radionuclides,[65] which they sell in legitimate commercial transactions, so tracing material to the producer would not provide a basis for retaliation. If terrorists obtained material through theft, illicit purchase, or an inside job, it would be hard to assign malevolent intent to the country involved.

[60] "Statement of Rolf Mowatt-Larssen, Director of the Office of Intelligence and Counterintelligence, United States Department of Energy, before the Homeland Security and Governmental Affairs Committee, United States Senate, April 2, 2008," in U.S. Congress. Senate. Committee on Homeland Security and Governmental Affairs. Hearings. "Nuclear Terrorism: Assessing the Threat to the Homeland," April 2, 2008.

[61] Information provided by Department of Homeland Security, email, May 17, 2010.

[62] See International Atomic Energy Agency, "International Catalogue of Sealed Radioactive Sources and Devices (ICSRS)"; and U.S. Nuclear Regulatory Commission. "Sealed Source and Device Registry: Supplement for 10 CFR Part 35 Uses."

[63] Margaret Goldberg and Martha Finck, "International Data on Radiological Sources," Idaho National Laboratory, INL/CON-10-18939, Preprint, July 2010, p. 3, http://www.inl.gov/technicalpublications/Documents/4633185.pdf.

[64] Ibid.

[65] National Research Council. *Radiation Source Use and Replacement, Abbreviated Version*, p. 41.

Issues for Congress

Priority for Countering Radiological Terrorism

What priority should be given to countering radiological vs. other forms of terrorism? There are many contending arguments. (1) Despite concerns about terrorist interest in RDDs, no successful RDD attack has occurred. (2) Of nuclear, chemical, biological, and radiological weapons, the latter would arguably kill the fewest people. (3) Most planning, training, equipment, and supplies that would help respond to an RDD attack would be of use in other disasters as well, so it is difficult to determine the balance between funds to counter all hazards and those to counter RDDs only. (4) Since costs resulting from an RDD attack could be tens of billions of dollars, some measures directly relevant to an RDD attack, such as decontamination R&D and securing radioactive sources, may be cost-effective.

Domestic vs. Overseas Expenditures to Secure Radioactive Sources

Where are U.S. funds to secure radioactive sources most effectively spent? One argument is that it is better to spend money to secure domestic radiological sources because if they are illicitly obtained they could be used promptly in an RDD, avoiding the risk of detection in other countries and at U.S. ports of entry. This effort would be costly. Of course, it would also be costly to secure radiological sources in countries that could not do so without international assistance. On the other hand, funds spent securing sources overseas might offer a higher benefit-cost ratio in that many sources overseas may be less secure than U.S. sources. Further, expenditures to counter the RDD threat overseas could help safeguard U.S. facilities in other nations and could help avert RDD attacks on critical facilities and infrastructure that could cause economic disruption.

Radiation Detection Networks

While attention has focused on explosive-driven "dirty bombs," an unobtrusive RDD attack could go undetected for hours, giving material time to spread and to irradiate people. A distributed network of sensors to detect, locate, and identify radioactive material would address this issue. Sensors could be mounted on buildings, police cars, or surveillance cameras. Work is underway to develop radiation-detection chips to be incorporated into cell phones or other mobile devices.[66] What would it cost to develop a detector network and deploy it in major metropolitan areas? Would it be appropriate for the federal government to fund deployment of such networks, or would deployment be a state or local responsibility?

Preparing for Decontamination

The main cost of an RDD attack would be decontamination. Proper methods depend on the RDD material, its form, types of surfaces affected, and the required decontamination level.

[66] Benjamin Sutherland, "My Blackberry as a Bomb Sniffer?," *Newsweek*, September 27, 2008; Emil Venere and Elizabeth Gardner, "Cell Phone Sensors Detect Radiation to Thwart Nuclear Terrorism," Purdue University news release, January 22, 2008; and personal communication, Simon Labov, Associate Program Leader for Detection Systems, Lawrence Livermore National Laboratory, February 14, 2011.

Decontaminators should be aware of the best techniques. Prompt availability of relevant information, such as through FEMA's Lessons Learned Information Sharing,[67] would help. Decontamination would require the proper equipment and supplies. Has the government stockpiled the needed resources or arranged to have them manufactured quickly? What areas might future R&D pursue? What is the cost of decontamination vs. demolition and reconstruction? Techniques to decontaminate areas struck by an RDD would help decontaminate the much larger area struck by radioactive fallout from an IND.

Waste Disposition and RDDs

Many studies have considered how to dispose of nuclear waste. The possibility of an RDD attack adds urgency to the disposition of radioactive waste. Most sealed sources have no disposition pathway. Choosing a permanent disposition pathway would reduce the risk of terrorists obtaining this material. On a larger scale, decontamination would generate chemicals, water, and radioactive material. How would this waste be handled? If decontamination proved ineffective, an alternative would be to demolish contaminated buildings, generating much rubble. Where would it go? If buried, would it contaminate the water table? If it were to be buried out of state, would another state accept it? How would it be transported? Would states along the proposed route try to block transit? It would appear more efficient to plan in advance how to dispose of this rubble rather than deciding on a rushed basis postattack.

Materials Protection

The GTRI Domestic Materials Protection Program visits facilities requesting its service, examines the security situation, and installs security devices. It provides this service on a voluntary basis at no initial cost to the facilities. As of February 2011, it had "identified more than 2,700 vulnerable buildings … with high-priority radioactive material in the United States," had completed security enhancements at 251 of the buildings, "with the remainder aiming to be completed by 2025."[68] Other upgrades will take several years as well. Alternatives include expanding this program to complete upgrades sooner, maintaining it at its current level, eliminating it, or making it mandatory.

Radiological Forensics

Congress has given nuclear forensics strong support, so it may wish to strengthen radiological forensics capability. Since radiological forensics is typically grouped with nuclear forensics, Congress could establish a panel to examine the unique aspects and requirements of the former and how its science and technology might be advanced. Congress could also support the buildout of archives of samples relevant to RDDs.

[67] U.S. Department of Homeland Security. Federal Emergency Management Agency. "Lessons Learned Information Sharing," https://www.llis.dhs.gov/index.do.

[68] U.S. Department of Energy. National Nuclear Security Administration. "NNSA: Securing Domestic Radioactive Material," fact sheet, February 1, 2011, p. 2.

Author Contact Information

Jonathan Medalia
Specialist in Nuclear Weapons Policy
jmedalia@crs.loc.gov, 7-7632