2

Nuclear and Radiological Threats

THE NUCLEAR AND RADIOLOGICAL THREAT MATRIX

For the purposes of the following discussion, the threats to homeland security from nuclear and radiological terrorism are grouped into the following three categories:

1. *Stolen state-owned nuclear weapons or weapons components,* modified as necessary to permit terrorist use.
2. *Improvised nuclear devices* (INDs) fabricated from stolen or diverted special nuclear material (SNM)[1]—plutonium and, especially, highly enriched uranium (HEU).[2]
3. Attacks on *nuclear reactors* or *spent nuclear fuel* or attacks involving *radiological devices*.

The threat matrix is summarized in Table 2.1 and is discussed in more detail below.

State-Owned Nuclear Weapons or Weapons Components

Several countries possess nuclear weapons that could potentially be turned to terrorist use: Britain, China, France, India, Israel, Pakistan, Russia, and the United States. Other countries have had weapons development programs in the past, and

[1]Special nuclear material includes fissile isotopes such as uranium-233, uranium-235, and plutonium-239 that can be used to make nuclear weapons.

[2]HEU contains ≥20 percent by weight of uranium-235.

one of these (South Africa's) led to the development of nuclear weapons. Iran, Iraq, and North Korea are believed to have active weapons development programs at present, and these countries probably have the technical capabilities to develop nuclear weapons but may not have sufficient quantities of SNM (plutonium or HEU).

The weapons arsenals of Britain, China, France, Israel, and the United States are probably well protected. Indian and Pakistani nuclear weapons are also thought to be adequately protected at present, but the near-term (1- to 5-year) security of Pakistani weapons may be problematical. Theft or diversion of Russian nuclear weapons for terrorist use may represent a significant near-term threat to the United States, especially the theft or diversion of smaller, man-portable weapons. Table 2.1 and the classified annex provide additional details on these threats.[3]

Improvised Nuclear Devices

Improvised nuclear devices are nuclear weapons fabricated by terrorists, with or without state assistance, using stolen or diverted SNM. The basic technical information needed to construct a workable nuclear device is readily available in the open literature. The primary impediment that prevents countries or technically competent terrorist groups from developing nuclear weapons is the availability of SNM, especially HEU.

HEU could potentially be obtained by terrorists from several sources. There are large stockpiles of excess HEU and weapons-grade plutonium in both the United States and Russia, and other countries with nuclear weapons may have smaller stockpiles of these materials. HEU also exists in nuclear fuel from naval reactors, and large stocks of reactor-grade plutonium are contained in commercial spent fuel. Spent-fuel reprocessing programs and separated stocks of reactor-grade plutonium also exist in several countries, and these stocks are routinely transported across national borders. Reactor-grade plutonium can be used to fabricate workable nuclear devices.

Theft or diversion of excess Russian HEU for terrorist use represents a significant near-term threat to the United States. There are estimated to be about 150 metric tons of separated plutonium and 1,200 metric tons of HEU in Russia. The United States has been working with Russia over the past 7 years to secure this material and has made major progress. These safeguards are effective against casual thefts but may not be effective against higher-level threats, especially sophisticated insider threats. Moreover, a complete inventory of Russian materials is not available, so it is impossible to confirm that diversions of materials have

[3]In addition to the unclassified discussion of nuclear and radiological terrorism provided in this chapter, a classified annex containing further treatment of these topics has been produced by the study.

not already occurred. Additionally, there have been more than a dozen seizures of SNM from Russia and surrounding countries since the early 1990s. Most of the seized materials are thought to have been smuggled from Russian civilian nuclear sites.

Stocks of SNM also could be produced clandestinely, either through enrichment of uranium or reprocessing of spent nuclear fuel to recover plutonium. Uranium enrichment is equipment intensive and time consuming, and detection is increasingly likely as the scale of operations is increased. A small-scale program could potentially be hidden through careful facility design, however, and could, in principle, produce sufficient material for a weapon if operated for several years. Reprocessing to recover plutonium also can be carried out in small, difficult-to-detect facilities but requires access to irradiated reactor fuel. Any country with a research reactor has potential access to such fuel, and there are, in addition, large stocks of spent fuel in power reactors in countries of the former Soviet Union and also in foreign research reactors, some of which still operate with HEU. Clandestine production of SNM by states or terrorist groups for use against the United States represents a significant near-term threat to homeland security.

Nuclear Reactors, Spent Nuclear Fuel, or Radiological Dispersion Devices

The threats considered here include attacks on nuclear power plants (both commercial nuclear power plants (NPPs) and research reactors), their spent fuel storage facilities, and spent fuel transportation casks; detonation of conventional explosive devices packed with radioactive materials, so-called "dirty bombs;" and the surreptitious placement of radiation sources in places frequented by large numbers of the public. Attacks on DOE-owned nuclear facilities were not considered because these are generally considered to be hardened and well protected.

Nuclear Power Plants

The United States has 103 operating civilian nuclear power reactors at 65 sites that generate about 20 percent of the U.S. electrical supply (USNRC, 2002; EIA, 2002). The U.S. Nuclear Regulatory Commission (USNRC) regulates NPPs and has had a long-standing concern about security and safeguards. The agency's security and safeguards regulations are extensive and actively enforced.

The USNRC requires that NPPs be protected against a "design basis threat," defined at present to involve a ground attack by a group consisting of several armed terrorists aided by an inside collaborator.[4] NPPs are required to train their

[4]Additionally, some NPPs located near airports have been designed to withstand certain types of low-speed takeoff and landing accidents involving aircraft in common use when the plants were licensed in the 1970s.

TABLE 2.1 The Nuclear and Radiological Threat Matrix

TABLE 2.1A State-Owned Nuclear Weapons

Threat Category	Threat Description	Threat Level	Potential Consequences	Probability of Occurrer
State-owned nuclear weapons	Theft and diversion of state-owned nuclear weapons for use, with or without modification, against U.S. targets or assets	United States: Low—weapons are well protected and tactical weapons have integrated permissive action links to prevent unauthorized use Britain, China, France, Israel: Low—weapons are few in number relative to U.S.-Russian arsenals and are well protected Pakistan, India: Medium—weapons are under secure control of the military, but political situation is unstable Russia: Medium—large numbers of weapons with poor inventory controls	Potentially catastrophic—massive loss of life and severe political and economic destruction possible	Moderate 5 years, w potential f

security personnel against this threat and are periodically tested by the USNRC to ensure readiness to meet this threat.

The current design basis threat for NPPs does not include high-speed attacks with fully loaded civilian airliners or, alternatively, smaller general aviation aircraft loaded with high explosives (HE) or attacks from the ground using HE projectiles. Potential targets for aircraft or ground attacks against an NPP are described in the classified annex.

The USNRC is supporting work at the Sandia National Laboratories, and the nuclear industry's trade association, the Nuclear Energy Institute (NEI), is directing work at the Electric Power Research Institute (EPRI) to assess some of these threats. These studies, which involve modeling aircraft impacts against steel-reinforced concrete structures and investigating the potential effects of aircraft-fuel fires, are proceeding independently of each other and will not be completed until after this report is published.

The details of these studies are classified and/or sensitive, and the results are

ces	Probability of Occurrence	Technical and Policy Challenges	Approaches to Mitigation
ic— ss of life political mic possible	Moderate over the next 5 years, with a high potential for surprise	Theft or diversion may not require state assistance and may go undetected if theft occurs in Russia Stolen or diverted weapons could be converted for terrorist use HEU-based weapons smuggled into the United States could be difficult to detect and recover First responders may be killed or incapacitated by attack	Improve indications and warnings capabilities Improve security of Russian and Pakistani nuclear weapons at storage sites and borders Accelerate deployment of sensor arrays at critical U.S. entry points and targets Develop and announce policies to deter use of weapons by terrorist states Improve attribution capabilities

preliminary. But taken together, these studies suggest that a terrorist attack on an NPP could have potentially severe consequences if the attack were large enough. The severity is highly dependent on the specific design configuration of the NPP, including details such as the location of specific safety equipment. Additional details are provided in the classified annex.

The potential vulnerabilities of NPPs to terrorist attack seem to have captured the imagination of the public and the media, perhaps because of a perception that a successful attack could harm large populations and have severe economic and environmental consequences. There are, however, many other types of large industrial facilities that are potentially vulnerable to attack, for example, petroleum refineries, chemical plants, and oil and liquefied natural gas supertankers. These facilities do not have the robust construction and security features characteristic of NPPs, and many are located near highly populated urban areas. The committee has not performed a detailed examination of the vulnerabilities of these other types of industrial facilities and does not know how they compare to

TABLE 2.1B Improvised Nuclear Devices

Threat Category	Threat Description	Threat Level	Potential Consequences	Probability of Occurrer
Improvised nuclear devices	Theft or diversion of SNM for fabrication of nuclear devices for use against U.S.targets or assets	United States: Low—SNM is well protected Britain, China, France, India, Israel, Pakistan: Low—small amounts of materials are well protected Russia: High—large inventories of SNM are stored at many sites that apparently lack inventory controls ,and indigenous threats have increased	Potentially catastrophic—massive loss of life and severe political and economic destruction possible	Moderate 5 years, w potential f

the vulnerabilities of NPPs. It is not clear whether the vulnerabilities of NPPs constitute a higher risk to society than the vulnerabilities of other industrial facilities.

Research Reactors

Research reactors are used primarily to produce neutrons and gamma rays for research and development, and they provide a testbed for education on reactor physics and operations. As of April 2002 there were 36 operating research reactors in 23 states, an additional 12 reactors were being decommissioned, and 7 had licenses only to possess radioactive material.[5] Most research reactors are

[5]Much of the factual information used in this section is taken from the USNRC Web site. See, particularly, <http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/research-reactors.html>, last accessed May 20, 2002.

ces	Probability of Occurrence	Technical and Policy Challenges	Approaches to Mitigation
ic— ss of life political mic possible	Moderate over the next 5 years, with a high potential for surprise	Theft or diversion may not require state assistance and may go undetected Crude HEU weapons could be fabricated without state assistance HEU-based INDs smuggled into the United States could be difficult to detect and recover First responders may be killed or incapacitated by attack	Improve indications and warnings capabilities Consolidate SNM at Russian sites, improve inventory controls, and improve security at sites and borders Accelerate blend-down of Russian HEU Accelerate the development and deployment of SNM sensor arrays at critical U.S. entry points and targets Improve capabilities for remote detection of HEU Develop and announce policies to deter use of INDs by terrorist- states Improve attribution capabilities

located at universities or government laboratories,[6] and many university research reactors operate on a restricted basis and therefore do not generate much radioactive material.

With thermal outputs ranging from about 0.1 to 20 megawatts, U.S. research reactors produce much less radiation, heat, and waste (e.g., spent fuel) than do power reactors, whose thermal output is commonly 2,000-3,000 megawatts. Research reactors also generally have fail-safe shutdown systems, and most do not generate sufficient heat to be vulnerable to core accidents, even in the event of a coolant loss. The potential consequences of terrorist attacks therefore appear to be small relative to power reactors.

[6]In addition, the Department of Energy and the U.S. Army operate research and test reactors at several of their sites. The thermal output of these reactors ranges from 5 to 400 megawatts. These reactors are not licensed by the USNRC and are not considered in this discussion.

TABLE 2.1C Radiological Attacks

Threat Category	Threat Description	Threat Level	Potential Consequences	Probability of Occurrer
Nuclear power plants (NPPs)	Ground or air assaults on civilian NPPs	High—Over 100 potential targets exist in the United States	Variable, ranging from reactor shutdowns to core meltdowns with very large releases of radioactivity	Potential f attacks is l near term
Research reactors	Ground or air assaults	High—there are 36 operating reactors	Little or no release of radioactivity likely	Unclear in
Spent nuclear fuel in wet or dry storage	Ground or air assaults on spent fuel pools or dry storage casks	High—Potential targets exist at all commercial NPP sites	Little or no release of radioactivity likely	Potential f attacks is l next 5 yea would be d locate or s damage
Radiological sources	Attacks with dirty bombs or placement of radioactive sources in public places	Very high—radiation sources are numerous and highly dispersed worldwide	Few deaths likely, but potential for economic disruption and panic is high	High—mat means are available, few prever in place
Radioactive waste	Same as for radiological sources	Very high—radioactive waste is abundant worldwide and not well protected	Trivial—most types of radioactive waste potentially available to terrorists have low specific activity	High—mat means are available, few prever in place

Spent Nuclear Fuel in Wet or Dry Storage

All civilian NPPs contain storage facilities for spent nuclear fuel and, with few exceptions, all of the spent fuel produced by those reactors is being stored at the sites where it was produced. Approximately 42,000 metric tons of spent fuel are currently stored under water in large spent fuel storage pools for cooling and shielding purposes. These pools are constructed of steel-reinforced concrete and are typically located adjacent to reactor containment buildings.

At some NPP sites spent nuclear fuel also is being stored outside the power-plant buildings in dry casks on concrete pads. At present, about 3,000 metric tons of spent fuel are being stored in this fashion. The casks are constructed of one or more layers of stainless steel and steel-reinforced concrete. The spent fuel is stored in the casks in an inert atmosphere at low pressure. A consortium of

ces	Probability of Occurrence	Technical and Policy Challenges	Approaches to Mitigation
ranging or to core with very ses of ty	Potential for 9/11-type attacks is high in the near term	Stopping airplane attacks that deliver large amounts of energy directly on target	Perform vulnerability analysis of NPPs Harden vulnerable NPPs and improve redundancies of critical safety systems
o release of ty likely	Unclear in the near term	Providing security against all types of attacks	Minimize the amount of fuel stored onsite
o release of ty likely	Potential for 9/11-type attacks is high over the next 5 years, but targets would be difficult to locate or severely damage	Stopping airplane attacks that deliver large amounts of energy directly on target	Perform vulnerability analysis of spent nuclear fuel storage sites Move vulnerable spent fuel in wet storage to dry cask storage
s likely, ial for disruption is high	High—materials and means are readily available, and there are few preventive measures in place	Training first responders to deal with these types of attacks	Improve first responder capabilities Improve public education
ost types tive waste available s have ic activity	High—materials and means are readily available, and there are few preventive measures in place	Training first responders to deal with these types of attacks	Improve first responder capabilities Improve public education

nuclear utility companies has applied to the USNRC for a license to construct a centralized dry-cask storage facility (the Private Fuel Storage Facility) in Utah west of Salt Lake City. This facility, if licensed and constructed, could house up to 40,000 metric tons of spent fuel contained in up to 4,000 above-ground storage casks on thick reinforced-concrete pads (Private Fuel Storage, 2002).

The threat of terrorist attacks on spent fuel storage facilities, like reactors, is highly dependent on design characteristics. Moreover, spent fuel generates orders of magnitude less heat than an operating reactor, so that emergency cooling of the fuel in the case of attack could probably be accomplished using low-tech measures that could be implemented without significant exposure of workers to radiation. Dry cask storage systems are very robust and would probably stand up to aircraft attacks as well.

Like dry storage casks, spent fuel transport containers are very robust and appear to offer similar protection against terrorist attack. Studies on the vulnerability of spent fuel transport containers to sabotage suggest that relatively little or no radioactivity would be released in the event of a terrorist attack, and the USNRC is now undertaking a package performance study that will examine fuel performance and source terms under a variety of impact situations. That agency is conducting a top-to-bottom review of potential vulnerabilities, including transport vulnerabilities, in the wake of September 11. In the meantime, it has issued advisories to its licensees to take additional precautions until these reviews are completed.

Radiation Sources and Radioactive Waste

A wide variety of radiation sources are used in the civilian economy for, among other things, industrial radiography, radiation therapy, university research, and natural resource exploration. The approximately 2 million sources licensed by the USNRC range in activity from millicuries to tens of kilocuries and typically contain penetrating gamma emitters like cesium-137, cobalt-60, and iridium-192; alpha emitters like radium-226 and americium-241; and beta emitters like strontium-90. Devices in which such sources are dispersed by explosives or other means are called radiological dispersion devices (RDDs).

In the United States, most radioactive sources are regulated by the USNRC or by states under agreement with that agency, and a materials license is required to possess such sources. Licensees are responsible for safeguarding these sources and returning them to the manufacturer or properly disposing of them when the sources are no longer needed. This system is not foolproof, however. For example, according to USNRC records, several hundred U.S. sources are unaccounted for and presumed lost.

Radioactive sources are also used widely in other countries, not all of which have the regulatory controls that exist in the United States. Control of sources may be a particular concern in some central and eastern European countries, which lack strong regulatory or accounting standards.[7]

The United States also produces quantities of radioactive waste that could potentially be used in an RDD. This waste includes high-level spent nuclear fuel and high-level defense waste stored at government or commercial sites; transuranic waste stored at government sites; and low-level industrial, research, and medical waste stored at commercial sites, universities, and hospitals. Low-level waste may be a particularly attractive terrorist target: It is produced by many companies, universities, and hospitals, it is not always stored or shipped under tight security, and it is routinely shipped across the country. Although labeled

[7]See Gonzalez (1999) for a recent review of lost and stolen radioactive sources.

"low-level," some of this waste has high levels of radioactivity and could potentially be used to make an effective terrorism device.

RDD attacks could be carried out in several ways. Nonexplosive sources could be hidden in facilities frequented by large numbers of the public (e.g., sports stadiums, subway systems) or dispersed in building ventilation systems. Additionally, a radiation source could be combined with an explosive to disperse radioactive contamination over areas on the order of hundreds of square meters to a few square kilometers, depending on meteorological conditions. A radioactive waste shipment also could be attacked while in transit. Although such an attack probably would not disperse large quantities of radioactivity, it could cause public panic, especially if the attack took place in a highly populated urban area.

Detailed studies of RDDs suggest that few if any human deaths would be expected from dispersed radiation, although the explosion itself could cause casualties. The presence of dispersed radioactivity in the attacked area could, however, confound rescue efforts. The most severe effects on human health are produced if the material can be efficiently dispersed in respirable form. For optimum particulate sizes, inhaled material can remain lodged in the lungs, leading to either acute or chronic effects, depending on the amount and type of material respired. Although there are methods to construct an RDD to obtain good dispersion of inhalable particles, they require expert knowledge and access to university-level laboratory facilities.

HOMELAND SECURITY CHALLENGES

The threat matrix presented in Table 2.1 and discussed in previous sections suggests that the United States faces several near-term (1-5 year) vulnerabilities to terrorist acts using nuclear and radiological dispersal weapons. Several potential vulnerabilities are described in this section.

State-Owned Nuclear Weapons and Improvised Nuclear Devices

At present, the United States has no evidence that a terrorist organization or nonnuclear state possesses stolen nuclear weapons or INDs. However, this situation could change rapidly over the near term if steps are not taken to better secure nuclear weapons and SNM, especially in Russia. In the future, efforts to develop INDs may involve virtual collaborations among groups of countries and terrorist organizations. These efforts will be harder to detect and interdict because the different materials, facilities, activities, and expertise will be spread across large and unconnected geographical areas. As noted above, the primary impediment to the success of IND development efforts is the availability of SNM, especially HEU. The first challenge, then, for the United States and its allies is to improve security for weapons and special nuclear material wherever they exist, but especially in Russia.

Once a terrorist state or organization is able to procure a state-owned nuclear weapon or SNM, especially HEU, it will be able to fabricate an IND if it has the appropriate technical expertise. In addition to the potential for obtaining SNM from existing stocks in countries like Russia, the technologies for making SNM are ubiquitous, and past experiences, which are discussed in the classified annex, illustrate the difficulty of detecting well-concealed clandestine efforts to produce these materials. Therefore, the second challenge for the United States and its allies is to improve the gathering of indications-and-warnings intelligence on efforts by states or groups to obtain a nuclear capability so that resources can be focused on countering the most significant threats. The third challenge is to improve capabilities for detecting and interdicting stolen nuclear weapons and INDs once they are obtained by a terrorist group or state.

The consequences of terrorist use of a stolen weapon or IND are horrible to contemplate. A successful detonation of a stolen weapon or IND could produce massive casualties and cause substantial damage to the nation's political and economic infrastructure. Although recovery would eventually occur, it would be both expensive and lengthy. While recovery plans should be put into place to deal with such attacks, the main focus of the nation's efforts must be on prevention of attacks by whatever means possible.

Nuclear Reactors, Spent Nuclear Fuel, and Radiological Dispersion Devices

Nuclear power plants may present a tempting high-visibility target for terrorist attack, and the potential for a September 11-type surprise attack in the near term using U.S. assets such as airplanes appears to be high. Such attacks could potentially have severe consequences if the attack were large enough and, were such an attack successfully carried out, could do great harm to the nation's near-term energy security and civilian nuclear power as a long-term energy option.

Complete denial of the means to attack NPPs from the air or ground using U.S. assets such as aircraft is probably not feasible. If important vulnerabilities are identified, however, design and operational fixes exist, some of which are easily identifiable, that could substantially harden the facilities. Some of these possible fixes are discussed in the classified annex.

The private ownership and operation of NPPs present some additional challenges. One involves cost, and another information sharing. Private companies may be hesitant to commit significant resources to reducing vulnerabilities unless they receive clear guidance and leadership from the USNRC. Further, operators may be unable to pass such costs on to consumers in a highly competitive electricity market. This has important ramifications for nuclear energy as a long-term contributor to the U.S. energy supply. Information sharing between government agencies and plant owners and operators on potential vulnerabilities and operational fixes is essential for improving security at the nation's NPPs. Such infor-

mation sharing is currently problematical, however, because much of the information to be shared is classified.

Of course, the development of remedies for reducing potential NPP vulnerabilities to terrorist attack must consider both *costs* and *achieved risk reductions*, especially in view of the potential vulnerabilities of other types of industrial facilities, as discussed elsewhere in this chapter. The nation's resources to address these vulnerabilities are limited and thus have to be expended in a way that achieves the greatest risk reduction at the lowest overall cost to society.

Given the wide use of radiation sources in the United States and other countries, a determined terrorist would probably have little trouble obtaining material for use in an RDD. Fortunately, many radiation sources are strong gamma emitters and, unless heavily shielded, can be readily detected with existing sensor technologies. If an RDD attack were to occur, the casualty rate would likely be low, and contamination could be detected and removed from the environment, although such cleanup would probably be expensive and time consuming.

It is clear that the aim of an RDD attack would be to spread fear and panic and to cause as much disruption to society as possible. Given the public fear of anything "nuclear" or "radioactive," even a minor terrorist attack could have greatly magnified psychological and economic consequences. The ease of recovery from an RDD attack would depend to a great extent on how the attack was handled by first responders, political leaders, and the news media, all of which would help to shape public opinion and reactions.

REDUCING VULNERABILITIES

Several steps can be taken over the near term to reduce the nation's vulnerability to acts of nuclear and radiological terror. Science and technology have an important role to play in this effort but clearly are insufficient in themselves to meet the future challenges. Policy and procedural changes may also be required, as described in the following discussion.

Stolen Nuclear Weapons and Improvised Nuclear Devices

There are no obvious technological silver bullets to reduce the nation's vulnerability to terrorist use of stolen nuclear weapons or INDs. Nevertheless, science and technology can play a central role in an *enduring, multilayered homeland-defense system* that provides for the following capabilities:

- Indications and warnings of terrorist group membership, structure, intentions, and transformational activities;
- Accounting of and security for weapons and SNM inventories at their sources;

- Detection and interdiction, using technology and intelligence, of weapons and SNM moved across national borders, especially Russian and U.S. borders;
- Detection of weapon or IND movements inside the United States;
- Effective responses to nuclear and radiological attacks if they do occur; and
- Attribution to identify weapons and/or SNM characteristics and sources of origin.

Such a system must be structured to overcome the political inertia that inevitably develops over time and that can lead to a slackening of effort. A good example of such inertia is the federal government's reduced willingness to provide funding during the last decade to the Federal Aviation Administration (FAA) for air marshals to guard commercial flights against hijackers. It appears that the FAA's effectiveness in reducing airline hijackings through the 1980s led to a perception that the risk of hijacking no longer existed.

Protection, Control, and Accounting of Nuclear Weapons and Special Nuclear Material

Nuclear weapons and SNM can be most effectively protected, controlled, and accounted for at their sources, which are relatively few in number compared with the many potential points of transit across national borders and are protected by state-run security infrastructures. Therefore, the first line of homeland defense against nuclear and radiological terrorism is a robust system for protecting, controlling, and accounting for nuclear weapons and SNM at their sources.

Technology for weapons and SNM protection, control, and accounting already exists and has been deployed in many nuclear countries. The impediments to more widespread deployment of these technologies in nuclear weapons and SNM states include cultural differences over what constitutes workable and acceptable technologies; funding for procurement, training, and security screening of the necessary personnel; and the willingness of states to accept and deploy such systems.

Of particular concern is the deployment of these systems in Russia, which possesses large stockpiles of weapons and SNM, and Pakistan, whose weapons are controlled in a fashion that may be unpredictable, especially given the potentially unstable governmental situation. The United States can—and should—engage nuclear weapons states, states possessing SNM, and the International Atomic Energy Agency (IAEA) in bilateral and multilateral discussions aimed at improving the protection, control of, and accounting for weapons and SNM. To this end, the following four actions should be taken:

Recommendation 2.1: The U.S. government, working through the Department of Energy, Department of Defense, and Department of State, should

increase the urgency and pace of discussions with states possessing nuclear weapons and special nuclear material with the goal of identifying and implementing more effective safeguards through the wider deployment of protection, control, and accounting technologies.

Although the United States has technically sophisticated capabilities to offer to other nations, other nations have also identified good technical solutions to many of these challenges. Technology sharing is essential for preventing the unauthorized procurement and use of nuclear weapons.

Recommendation 2.2: Concurrently, the U.S. government, working through the Department of Energy and Department of Defense, should reexamine the security of its own nuclear weapons, both within its borders and elsewhere.

Stolen U.S. nuclear weapons represent a very small threat in the universe of threats described in this chapter; nevertheless, protecting these weapons is solely the responsibility of the U.S. government, and a reexamination to determine their security would set a positive example for other nuclear powers to emulate. In particular, the risks and benefits of retaining forward-based nuclear weapons in NATO countries should be reassessed, especially in light of the 2001 Nuclear Posture Review, which emphasizes that the addition of non-nuclear strike forces to the U.S. deterrent capability will reduce U.S. dependence on nuclear forces.[8] Although the presence of forward-based nuclear weapons in NATO countries does not pose an immediate danger given current levels of security and protection measures, the potential for rapid, regional changes in the geopolitical security environment is cause for concern.

Recommendation 2.3: The U.S. government, working through the Department of Energy and Department of Defense, should undertake an internal evaluation of its bilateral Materials Protection, Control, and Accounting (MPC&A) program in Russia and consider ways to accelerate progress in safeguarding nuclear weapons and special nuclear materials, especially to counter potential insider threats. A principal goal of this evaluation should be to identify ways to accelerate deployments of means to safeguard (1) atomic demolition munitions and other small nuclear warheads and (2) special nuclear material, particularly highly enriched uranium.

This program is moving at an irregular and sometimes interrupted rate for a variety of reasons, but there are several actions the United States could take to

---

[8]Transmittal letter of the 2001 Nuclear Posture Review to Congress, signed by Donald H. Rumsfeld. The classified review was completed in December 2001. There are other technical and diplomatic issues relevant to the nuclear posture that would have to be considered in this reassessment, including binding agreements with NATO countries.

improve its reach and effectiveness. These include (1) encouraging more of the work under this program to take place through direct scientist-to-scientist contacts; this may help to promote a better understanding of workable approaches for both countries and (2) reconceptualizing the program as a fully joint program of technology research, development, and deployment[9] that can serve to improve Russian security and raise worldwide safeguard norms.

The first essential step in a robust MPC&A program is an accurate estimate of SNM inventories, which appears to be lacking in Russia. To address this problem, the United States should work with the Russian government to obtain an accurate inventory of its weapons-usable materials to match the U.S. declaration (DOE, 1994, 1996, 1998) in a way that addresses Russian national security concerns.[10]

Recommendation 2.4: The U.S. government, working through the Department of Energy, should increase the priority and pace of cooperative efforts with Russia to safeguard its highly enriched uranium by blending down this material as soon as possible.

One way to accomplish this objective is to encourage Russia to down-blend HEU in two stages: the first to just less than 20 weight percent to eliminate the proliferation threat, and the second to those levels (typically 4 to 5 percent) required for sale as feed for reactor fuel. This two-stage approach would not require any more time or effort than the one-stage process used at present,[11] and the first stage probably could be accomplished in about 2 years if adequate funding were made available.

Recommendation 2.5: The U.S. government, working through the Department of State, Department of Energy, and U.S. Nuclear Regulatory Commission, should provide encouragement as well as technical and financial assistance to the International Atomic Energy Agency to raise the levels of

---

[9]This effort could involve scientists and engineers from both countries, and one of its explicit goals could be to improve protection, control, and accounting technologies and practices and to share these improvements with other countries and organizations, especially the International Atomic Energy Agency.

[10]For example, the Russian government could make a secret declaration, certify to the United States that such a declaration had been made, and provide the declared inventories to the U.S. government in encrypted form as evidence of this certification. The Russian government would hold the encryption key and might, at some time in the future, make that key public so that the inventory could be verified.

[11]The same uranium hexafluoride (UF_6) gas flow would blend four times as much uranium-235 to 20 weight percent as to 4.4 percent, and the down-blending facility in Russia could handle at least twice the current gas flow. Furthermore, accelerating the pace of down-blending would not disrupt world uranium markets, because the availability of 4.4 percent uranium-235 for nuclear fuel is limited by its rate of sale by Russia to world markets and not by the rate of down-blending. Accelerating the pace of down-blending may require international cooperation beyond that of the United States.

international norms for protecting civilian special nuclear materials, specifically highly enriched uranium from research reactors and civilian plutonium from intact and reprocessed spent nuclear fuel.

The assistance could include technical support and funding for safeguards-technology development and deployment activities. The United States also should encourage other nuclear states to provide support for this effort.

Detection and Interdiction of Illicit Weapons and Special Nuclear Material

An important line of defense in a layered system of homeland protection is the detection and interdiction of illicit nuclear weapons and SNM as well as the detection and disruption of illicit weapons development programs. Science and technology can contribute to this defense effort in at least two ways: (1) by providing technical means for detecting the movement of SNM, especially HEU, either in weapons or as contraband, through border transit points and around critical U.S. assets such as ports, cities, and other high-value facilities; and (2) by providing sophisticated data-mining tools for analysis of intelligence on nuclear smuggling and on illicit weapons development programs.

The presence of certain types of penetrating radiation is a signature of most (but not all) SNM. Passive detection of gamma rays and/or neutrons can be an effective screening technique in some circumstances for revealing the presence of illicit SNM or INDs. In other cases, active interrogation methods may be required. While shielding can reduce these signals, they can serve as a useful first indicator of SNM, as well as other radioactive materials that could pose threats.

The nuclear materials of primary interest in weapons and INDs are plutonium, primarily plutonium-239 and plutonium-240, and HEU. Plutonium can be detected through passive gamma-ray and neutron monitoring, but HEU is difficult to detect passively owing to its low specific activity, low spontaneous fission rate, and low-energy gamma-ray emissions. Passive monitoring of these materials requires large-area detectors and relatively long exposure durations for acceptable sensitivity. HEU can be detected by active monitoring using, for example, neutron detectors and pulsed neutron sources. Additionally, both HEU and plutonium can be detected indirectly by gamma radiography, which is sensitive to high-atomic-number materials. Active systems are more complex and costly than passive detectors, however, and they emit radiation. Consequently, there may be radiological safety issues associated with their use in populated areas.

The full deployment of a national detection network would be an expensive proposition given the large numbers of international transit points, entry points into the United States, and critical U.S. cities and facilities. Although sensor technologies now exist for such deployments, it will be a daunting technical challenge to integrate these technologies into effective and reliable detection systems—in particular, to sort through the thousands of hits that would be re-

ceived each hour from legitimate transport of commercial radioisotopes (including isotopes implanted or injected into people for medical tests and treatments), identify and track suspicious targets while the threats they pose are being evaluated, and dispatch responders to interdict the target if the threat proves credible, all in real time. A poorly designed system would likely be turned off or ignored by frustrated operators and responders once the false alarms reached even moderate levels. The state of the art for such detection systems has not yet advanced to the levels needed to make a national deployment feasible.

A careful analysis of likely SNM transport routes, however, would likely reveal a smaller number of choke points where well-designed detection systems could be effectively deployed. Such choke points might include the following:

- Critical border transit points in countries like Russia;
- Major global cargo-container ports, especially at cargo entry and transfer portals;
- Major U.S. airports with large numbers of international arrivals;
- Major choke points in the U.S. interstate highway system—for example, through the Rocky Mountains; and
- Major roadways, bridges, and tunnels into critical U.S. cities.

The deployment of sensor systems even at a large number of such choke points would not guarantee the detection of SNM in transit—determined terrorists probably could find ways to overcome such systems by using secondary entry points and roads or by using heavy shielding. But the deployment of a well-tested, national integrated detection network would be a powerful component of the layered homeland defense system.

A national detection network could consist of several types of sensors: large numbers of simple counters that indicate the presence of radiation, backed up by smaller numbers of spectroscopic instruments to identify specific isotopic signatures. The technical challenge for the deployment of both types of sensors is the differentiation of signals of interest from the background of naturally occurring radioactivity and medical and industrial radioisotopes. There is a surprising lack of comprehensive data on the normal variations in background and radioactivity in general commerce.

Small hand-held (“pager”) radiation detectors are becoming available to customs officials, police, and first responders. These instruments could form the first layer of detection defense for illicit radioisotopes (especially strong gamma emitters) and could also be used by emergency personnel when responding to suspected radiological incidents. At present, most of these instruments have no spectroscopic discrimination capabilities; additional R&D would be needed to develop low-cost instruments of this type with spectroscopic capability and to improve their sensitivity and selectivity. Fixed instruments at airports or other

choke points can provide very useful sensitivity for materials in luggage or carried in truck cargo. R&D to support the innovative design and production of cost-effective detectors to meet these needs could be an important path to progress.

The following actions should be taken to improve the nation's capabilities to detect the illicit movement of weapons and SNM:

Recommendation 2.6: A focused and coordinated near-term effort should be made by the Department of Energy, through its National Nuclear Security Administration, and by the Department of Defense, through its Defense Threat Reduction Agency, to evaluate and improve the efficacy of special nuclear material detection systems that could be deployed at strategic choke points for homeland defense.

The objectives of these evaluations should be to provide (1) technical feedback to system developers that can be used to improve system design and performance; (2) improved definition of background signals at potential monitoring sites and radioisotopes in general commerce that can be used to improve system capabilities to detect illicit materials in transport; and (3) experience in detecting materials in transport that can be used to develop protocols for identifying false positives and evaluating and responding to actual threats.

Recommendation 2.7: Research and development support should be provided by the Department of Energy and Department of Defense for improving the technological capabilities of special nuclear material detection systems, especially for detecting highly enriched uranium.

In the near term, R&D is needed to improve neutron interrogation sources (i.e., neutron generators) and detector systems for HEU. Additionally, some priority should be given to the development of inexpensive portable detectors with spectroscopic discrimination capabilities so that such detector systems could be more widely deployed.

As mentioned above in this chapter, future efforts to develop INDs may be harder to detect and disrupt because such efforts are likely to involve multiple organizations spread across the globe. Detection of such efforts will require the ability to assemble intelligence data from many disparate sources and to find patterns and connectivity among large amounts of seemingly unrelated data. This will require the development of new databases, for example, databases that can be used to track and attribute smuggling efforts; enhancements to the connectivity of various kinds of databases (e.g., intelligence, immigration, law enforcement, signals intelligence, and imagery) to enable searching for relevant data; and the development of sophisticated data-mining tools and techniques that can identify transnational patterns and connections in the acquisition of know-how, technology, and materials for fabricating illicit weapons.

Effective Responses to Nuclear and Radiological Attacks

Responses to nuclear and radiological attacks fall into two distinct categories that could require very different types of governmental actions: (1) attacks involving the detonation of a nuclear weapon or IND and (2) attacks involving RDDs. The first type of attack would likely involve massive property destruction and loss of life, making it difficult to mount an effective emergency response, at least over the short term. An emergency response action lasting months to years might be required in the wake of such an attack. The second type of attack would likely involve localized loss of life and no immediate danger to surrounding populations or property, but the potential for misinformation and public panic would be high. An emergency response action lasting weeks to months might be required, although longer-term cleanup might be needed for large RDD attacks. The worst scenarios involving nuclear power plants fall somewhere between these two categories, but, as noted in the classified annex, studies have not yet determined how credible these scenarios are.

Responses to nuclear and radiological attacks are governed by the Federal Radiological Emergency Response Plan,[12] which establishes authorities and procedures for responding to "peacetime" radiological emergencies such as accidents at nuclear power plants. This plan devotes only three paragraphs to radiological sabotage and terrorism, giving the Federal Bureau of Investigation the lead for investigating such acts and calling on other agencies, especially the designated lead federal agency, to assist the bureau in its investigative mission. The plan concludes that acts of sabotage and terrorism should not be treated as separate types of emergencies but are simply a "complicating dimension" of the other types of emergencies.

The correctness of this conclusion seems questionable given the attacks that might be envisaged in light of September 11. A terrorist attack could be much larger in magnitude than other events anticipated under this emergency plan. Such an attack could require large numbers of rescuers and medical personnel trained to deal with radiological emergencies; the ability to manage large populations in contaminated urban areas for long periods of time, potentially years; the ability to predict in real time the spread of radioactive contamination in debris clouds and provide this information to potentially affected populations in real time so that appropriate actions can be taken; and timely and effective cleanup capabilities. The current plan does not appear to provide the guidance needed to ensure this type of response in the case of nuclear terrorist attack.

---

[12] *Federal Radiological Emergency Response Plan—Operational Plan,* published by the Federal Emergency Management Agency in the *Federal Register* on May 1, 1996, with a correction published on June 5, 1996. The plan is available online at <http://www.au.af.mil/au/awc/awcgate/frerp/frerp.htm>. Accessed on April 22, 2002.

Recommendation 2.8: Immediate steps should be taken by the Federal Emergency Management Agency to update the Federal Radiological Emergency Response Plan, or to develop a separate plan, to respond to nuclear and radiological terrorist attacks, especially an attack with a nuclear weapon on a U.S. city. This plan should, at a minimum, address the following needs: (1) rapid mobilization of nationwide medical resources to cope with burns, physical trauma, and poorly characterized outcomes of exposure to radiation; (2) rapid airlift of field hospitals to the affected area; (3) means to provide the affected public with basic information on protection against radiation and fallout; (4) technical procedures for decontaminating people, land, and buildings; and (5) protection of citizens and foreign nationals from vigilante attacks. This plan should be mock exercised and, if required, incident site monitoring capabilities should be enhanced. Steps also should be taken to ensure that federal decision makers are familiar with this plan.

Should a nuclear or radiological attack occur, response effectiveness could be enhanced through public education efforts carried out well in advance of a nuclear or radiological attack. These efforts could include the stocking of potassium iodide pills by individuals to reduce the potential for thyroid cancers from releases of radioactive iodine. Such efforts may increase the public's willingness to accept market-based recovery approaches for land use and permitted activities in regions that are contaminated at levels just a few times above background radiation levels.

Attribution to Identify Characteristics of Weapons and Special Nuclear Material and Their Sources of Origin

As the history of the Cold War has shown, the most effective defense against attacks with nuclear weapons is a policy of nuclear retaliation. This past success suggests that the United States may be able to deter some future state-supported or state-sponsored nuclear and radiological terrorist acts by announcing in advance that it will retaliate by whatever means deemed appropriate, including the use of nuclear weapons, against states and terrorist groups responsible for nuclear or radiological attacks against U.S. citizens or assets.[13] To be a useful deterrent, however, this doctrine would have to be formulated and announced in advance, and its credibility would depend in large part on the ability of the United States to demonstrate to the rest of the world that it has the technical means to attribute such attacks to states or terrorist groups.

---

[13]The analogy between the Cold War and post-September 11 worlds is imperfect in that terrorist activity is dispersed geographically and may not be politically motivated. A doctrine of assured retaliation probably would not deter fanatical terrorist groups, but it may discourage states from providing such groups with aid and comfort.

Attribution is a difficult technical challenge—ideally, one would want to know both the characteristics of the weapon used in the attack and its country of origin. The former can be determined through careful analysis of blast debris; the latter might be determined by linking this information with intelligence on thefts, smuggling, and weapons development efforts by states and terrorist groups developed through the data-mining techniques discussed above.

Efforts are under way by national laboratories to develop an attribution capability under the Defense Threat Reduction Agency (DTRA). The goal is to develop the capability to perform a postdetonation debris analysis and to draw conclusions on the design and performance after an attack. The technology for developing this capability exists but needs to be assembled, an effort that is expected to take several years.

Recommendation 2.9: Given the potential importance of attribution to deterring nuclear attacks, the Defense Threat Reduction Agency's efforts to develop a capability for identifying perpetrators of an attack should continue to declared operability as quickly as practical.

Reactors

The events of September 11 suggest that physical and operational changes at some NPPs may be needed to mitigate vulnerabilities to attacks from the air using a large commercial airliner or a smaller aircraft loaded with high explosives and, possibly, attacks from the ground using HE projectiles. The technical analyses that are now being carried out by the USNRC and EPRI to understand the effects of such attacks on reactor containment buildings and essential auxiliary facilities are critical to understanding the full magnitude of this threat to the nation's NPPs.

Recommendation 2.10: The ongoing U.S. Nuclear Regulatory Commission and Electric Power Research Institute assessments of nuclear power plant vulnerabilities to airliner attacks should be completed as soon as possible, and follow-on work to identify vulnerabilities on a plant-by-plant basis, including vulnerabilities to air attacks by small craft loaded with high explosives or to ground attacks by high-explosive projectiles, should be undertaken as soon as these initial studies are completed. This "completion" should not stand in the way of early actions to address significant plant vulnerabilities that are identified in the course of the ongoing Sandia National Laboratories and EPRI assessments. If these assessments continue to show that important vulnerabilities exist, then steps should be taken to reduce such vulnerabilities as soon as possible.

If the USNRC discovers significant vulnerabilities at its licensees' reactors as a result of these analyses, it could mandate a number of physical and opera-

tional changes to reduce vulnerabilities to and the consequences of attacks. Some possible changes are listed in the classified annex. This list is by no means exhaustive, and an effective remedy can be applied at a particular reactor only after a careful analysis of risks and benefits, taking into account the comparative risk reduction that could be achieved by devoting resources to hardening nuclear plants versus other large industrial facilities.

Radiological Dispersion Devices

Although the damage potential of RDDs is far less than that of stolen nuclear weapons, improvised nuclear explosives, or successful attacks on reactors, the terror/panic potential of RDDs warrants increased attention to the control and use of radiological sources by regulatory agencies and materials licensees.

Recommendation 2.11: The U.S. Nuclear Regulatory Commission and the states with agreements with that agency should tighten regulations for obtaining and possessing radiological sources that could be used in terrorist attacks (i.e., large sources containing long-lived isotopes), including requirements for securing and tracking these sources. Additionally, licensees possessing large sources should be encouraged to substitute nonradioactive sources (compact accelerators, electron beams, and x-ray generators) when economically feasible.

Other important counters to RDDs are public education, emergency responder training, and preparation of leaders to deal quickly and effectively with terrorist acts. As noted above, the likely aim of an RDD attack would be to spread fear and panic and cause disruption. Recovery would therefore depend on how such an attack is handled by first responders, political leaders, the media, and general members of the public.

In general, public fear of radiation and radioactive materials appears to be disproportionate to the actual hazards. Although hazardous at high doses, ionizing radiation is a weak carcinogen, and its effects on biological systems are better known than those of most, if not all, toxic chemicals. Federal standards that limit human exposure to environmental ionizing radiation, which are based on the linear, nonthreshold dose-response relationship,[14] are conservative and protec-

[14]That is, mutagenic (cell mutation) and carcinognic (cancer) effects are assumed to increase linearly with radiation dose, with no threshold at low doses below which there is zero effect. A recent report by the National Council on Radiation Protection and Measurements concluded that "there is no conclusive evidence on which to reject the assumption of a linear-nonthreshold dose-response relationship for many of the risks attributable to low-level ionizing radiation . . ." (NCRP, 2001, p. 7).

tive, and the government continues to fund R&D[15] to improve scientific understanding of radiation effects on biological materials.

Education and training can serve as an effective counter to future RDD attacks. To this end, the committee recommends that the following actions be implemented:

Recommendation 2.12: Training should be provided to emergency responders (police, fire, and other emergency service personnel) on how to assess on-the-ground hazards from radiological attacks. As part of this training, responders should be provided with simple but effective radiation-monitoring devices, trained in their use, and told whom to contact for expert assistance, if needed. The Office of Homeland Security should take the lead for this effort in cooperation with the National Nuclear Security Administration and the Federal Emergency Management Agency.

Recommendation 2.13: Prepackaged kits of written materials on basic radiation science and effects should be developed for the media and national, state, and local leaders to help them respond appropriately to radiological attacks. The Office of Homeland Security should take the lead for this effort and should work with independent credible organizations to develop these kits.

Recommendation 2.14: A technically credible spokesperson at the national level who is perceived as being outside the political arena—for example, the President's Science Advisor, the Surgeon General, or their designated spokespersons—should be prepared to provide accurate and usable information to the media and public concerning public health and safety risks and appropriate response actions in the aftermath of a nuclear or radiological attack.

Such a response needs to be prepared and rehearsed in advance to avoid the kind of national leadership confusion that followed the anthrax attacks on Washington, D.C., in 2001.

---

[15]The Department of Energy sponsors research on low-dose radiation effects within the Office of Science and also supports the Radiation Effects Research Foundation, which is conducting a long-term longitudinal study of Japanese atomic bomb survivors. Additionally, the federal government provides funding to the National Research Council's Biological Effects of Ionizing Radiation (BEIR) Committees for periodic reassessments of low-dose health effects. The BEIR-VII study is currently in progress, and its objective is to determine the mathematical relationship between health risks and radiation dose for low levels of ionizing radiation.

CONCLUDING DISCUSSION

Many of the recommendations offered in this chapter call for an organized, focused, and adequately funded R&D effort to counter nuclear and radiological terrorism, as well as additional scientific, technical, and policy actions to reduce the nation's vulnerability to terrorist attacks, sometimes in cooperation with other national governments. To be effective, these efforts must bring to bear the best scientific and technical resources available to the federal government and must be well coordinated with other federal R&D and counterterrorism activities.

Important progress is already being made by the R&D and policy communities to reduce the nation's vulnerability to nuclear and radiological terrorism. There is not much evidence, however, that the R&D activities are being coordinated, that thought is being given to prioritizing these activities against other national counterterrorism needs, or that effective mechanisms are in place to transfer the results of these activities into application. Presumably the newly established Office of Homeland Security will take a lead role in the national counterterrorism effort, but that office does not have the expertise or budget to oversee a broad R&D effort.

The effectiveness of the nation's counterterrorism efforts could be improved if one agency were given the lead responsibility for coordinating and prioritizing, in consultation with other interested agencies, nuclear and radiological counterterrorism R&D. Several federal agencies have R&D responsibilities and could potentially take the lead: DOE's National Nuclear Security Administration (NNSA) already has a large R&D effort on many of the issues addressed in this chapter and is carrying out that work at the three national laboratories under its control.[16] The DOD's DTRA is carrying out R&D work to reduce threats from chemical, biological, and nuclear weapons of mass destruction. This work is being carried out primarily by DOD contractors, including NNSA national laboratories. The USNRC also sponsors R&D on NPP safety and vulnerabilities, and some of this work is carried out at NNSA national laboratories.

Given its large budget and broad scope of current work, it appears that DOE-NNSA is best positioned to take a lead role for R&D on nuclear and radiological terrorism. The committee, however, has not had an opportunity to study this issue in detail, especially to examine the current R&D portfolios of NNSA and DTRA or their strategic planning documents. The President's science advisor, working with DOE, DOD, USNRC, and other agencies with a stake in this decision, may be in the best position to develop a recommendation to the President regarding which agency should take a lead role in this important R&D effort. The designation of a lead agency also will require approval from the U.S. Congress.

---

[16]Lawrence Livermore National Laboratory, Los Alamos National Laboratory, and Sandia National Laboratories.

Recommendation 2.15: A single federal agency, possibly the Department of Energy's National Nuclear Security Administration, should be designated as the nation's lead research and development agency for nuclear and radiological counterterrorism. This agency should develop a focused and adequately funded research and development program to fulfill this mission and should work with other federal agencies, the President's science advisor, and the director of the Office of Homeland Security to coordinate this work and ensure that effective mechanisms are in place for the timely transfer of results to the homeland defense effort.

The centralization of lead R&D responsibilities into a single federal agency is no guarantee of success absent commitments to certain operating principles. Among these are commitments to appoint a technically capable staff to manage the R&D work; to provide sufficient and sustained funding to carry out an adequate program; and to reach across agency boundaries and outside government to obtain the expertise needed to execute the work and to ensure that results are moved expeditiously into application. While the events of September 11 appear to have produced a renewed sense of cooperation among federal agencies, the challenge for whichever agency is selected to lead this important R&D effort will be to nurture and sustain this spirit.

REFERENCES

Department of Energy. 1994. *Openness Press Conference Fact Sheets*, Office of the Press Secretary, Washington, D.C.

Department of Energy. 1996. *Plutonium: The First 50 Years,* Washington, D.C., 82 pp.

Department of Energy. 1998. *Commercial Nuclear Fuel from U.S. and Russian Surplus Defense Inventories: Materials, Policies, and Market Effects,* DOE/EIA-0619, Energy Information Administration, Washington, D.C., 115 pp.

Energy Information Administration. 2002. *U.S. Nuclear Generation of Electricity*. Available online at <http://www.eia.doe.gov/cneaf/nuclear/page/nuc_generation /gensum.html>.

Gonzalez, A.J. 1999. "Strengthening the Safety of Radiation Sources and the Security of Radioactive Materials: Timely Action," *IAEA Bulletin*, Vol. 41, No. 3, pp. 2-15.

National Council on Radiation Protection and Measurements. 2001. *Evaluation of the Linear-Nonthreshold Dose-Response Model for Ionizing Radiation*, Report No. 136. Bethesda, Md., 287 pp.

Private Fuel Storage. 2002. *The PFS Facility Specifications*. Available online at <http://privatefuelstorage.com/project/facility.html>.

U.S. Nuclear Regulatory Commission. 2002. *List of Power Reactor Units.* Available online at <http://www.nrc.gov/reactors/operating/list-power-reactor-units.html>.