

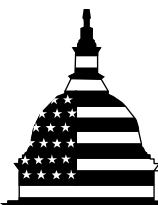
GAO

Report to the Chairman, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

September 2012

NUCLEAR NONPROLIFERATION

Additional Actions Needed to Improve Security of Radiological Sources at U.S. Medical Facilities



G A O

Accountability * Integrity * Reliability

Highlights of [GAO-12-925](#), a report to the Chairman, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

In the hands of terrorists, radiological material, such as cesium-137, could be used to construct a “dirty bomb.” Such material—encapsulated in steel or titanium and called a sealed source—is commonly found in equipment used by U.S. medical facilities to treat, among other things, cancer patients. NRC is responsible for regulating the commercial use of sealed sources and has relinquished its regulatory authority to 37 states, known as Agreement States. In 2008, NNSA established a program to provide security upgrades to U.S. hospitals and medical facilities that use radiological sources.

GAO was asked to determine (1) the extent to which NRC’s requirements ensure the security of radiological sources at U.S. medical facilities and (2) the status of NNSA’s efforts to improve the security of sources at these facilities. GAO reviewed relevant laws, regulations, and guidance; interviewed federal agency and state officials; and visited 26 hospitals and medical facilities in 7 states and Washington, D.C.

What GAO Recommends

GAO recommends, among other things, that NRC strengthen its security requirements by providing medical facilities with specific measures they must take to develop and sustain a more effective security program. NRC neither agreed nor disagreed with this recommendation and stated that its existing security requirements are adequate. GAO continues to believe that implementing its recommendation would contribute to increased security at U.S. hospitals and medical facilities.

View [GAO-12-925](#). For more information, contact Mark Gaffigan at (202) 512-3841 or gaffiganm@gao.gov.

NUCLEAR NONPROLIFERATION

Additional Actions Needed to Improve Security of Radiological Sources at U.S. Medical Facilities

What GAO Found

The Nuclear Regulatory Commission’s (NRC) requirements do not consistently ensure the security of high-risk radiological sources at the 26 selected hospitals and medical facilities GAO visited. One reason for this is that the requirements are broadly written and do not prescribe specific measures that hospitals and medical facilities must take to secure medical equipment containing sealed sources, such as the use of cameras or alarms. Rather, the requirements provide a general framework for what constitutes adequate security practices, which is implemented in various ways at different hospitals. Some of the medical equipment in the facilities visited was more vulnerable to potential tampering or theft than that of other facilities because some hospitals developed better security controls than others. Some examples of poor security GAO observed included: an irradiator, used for medical research and containing almost 2,000 curies of cesium-137, was stored on a wheeled pallet down the hall from, and accessible to, a loading dock at one facility; at a second facility, the combination to a locked door, which housed an irradiator containing 1,500 curies of cesium-137, was clearly written on the door frame; and at a third facility, an official told GAO that the number of people with unescorted access to the facility’s radiological sources was estimated to be at least 500. In addition, some NRC and Agreement State inspectors said the training NRC requires is not sufficient.

As of March 2012, the National Nuclear Security Administration (NNSA) had spent \$105 million to complete security upgrades at 321 of the 1,503 U.S. hospitals and medical facilities it identified as having high-risk radiological sources. Of the 26 hospitals and medical facilities that GAO visited, 13 had volunteered for the NNSA security upgrades and had received security upgrades, such as remote monitoring systems, surveillance cameras, enhanced security doors, iris scanners, motion detectors, and tamper alarms; three others were in the process of receiving upgrades. However, NNSA does not anticipate completing all such security upgrades until 2025, leaving a number of facilities potentially vulnerable. In addition, the program’s impact is limited because, among other things, it is voluntary, and facilities can decline to participate. To date, 14 facilities, including 4 in large urban areas, have declined to participate in the program. Combined, those 14 facilities have medical equipment containing over 41,000 curies of high-risk radiological material. According to police department officials in a major city, one hospital with a blood irradiator of approximately 1,700 curies has declined the NNSA upgrades due in part to cost concerns, even though the police department considers it to be a high-risk facility. GAO also found that NNSA is focusing the majority of the program’s resources on states with high curie amounts and large numbers of hospitals and medical facilities with high-risk radiological sources. However, some states with many hospitals and medical facilities have received fewer or no upgrades. While NNSA has conducted outreach efforts in partnership with NRC and Agreement States to encourage participation in its security upgrade program, there are still many facilities that are not participating in the program. The longer it takes to implement the security upgrades, the greater the risk that potentially dangerous radiological sources remain unsecured and could be used as terrorist weapons.

Contents

Letter		1
	Background	8
	NRC Requirements and Implementation by Licensees Do Not Ensure the Security of High-Risk Radiological Sources	10
	NNSA Completed Security Upgrades in More Than 300 Medical Facilities, but Some Hospitals Do Not Participate in the Voluntary Program	23
	Conclusions	35
	Recommendations for Executive Action	37
	Agency Comments and Our Evaluation	37
Appendix I	Scope and Methodology	42
Appendix II	NRC Security Controls and Selected Pending Part 37 Regulations Changes (10 C.F.R. Part 37)	45
Appendix III	Comments from the Nuclear Regulatory Commission	47
Appendix IV	GAO Contact and Staff Acknowledgments	51
Tables		
	Table 1: Breakdown of NNSA Total Costs for Domestic Material Protection Program, as of February 29, 2012	25
	Table 2: NNSA Expenditures on Assessments and Upgrades by State, as of March 1, 2012	32
Figures		
	Figure 1: Map of NRC Regions and 37 Agreement States	5
	Figure 2: Example of a Radioactive Sealed Source That Contains Americium-241	8
	Figure 3: Combination to Lock on Door Frame Outside Blood Bank	17
	Figure 4: Irradiator and Bank of Unsecured Windows Looking Out onto Loading Dock	18

Figure 5: NNSA-Installed Remote Monitoring System	26
Figure 6: NNSA-Installed Iris Scan with Hospital Card Reader	27
Figure 7: NNSA-Installed Security Camera	28
Figure 8: Irradiator with NNSA-Installed Tamper Alarm around Middle of Device	29

Abbreviations

DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
IAEA	International Atomic Energy Agency
IMPEP	Integrated Materials Performance Evaluation Program
LLNL	Lawrence Livermore National Laboratory
MML	Master Materials License
NNSA	National Nuclear Security Administration
NRC	Nuclear Regulatory Commission
NS-E	National Nuclear Security Administration (NNSA) Albuquerque Complex
NSTS	National Source Tracking System
OAS	Organization of Agreement States
ORNL	Oak Ridge National Laboratory
PNNL	Pacific Northwest National Laboratory
RSO	Radiation Safety Officer
SNL	Sandia National Laboratory
T&R	Trustworthiness and Reliability
VA	Department of Veterans Affairs
Y-12	Y-12 National Security Complex

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 10, 2012

The Honorable Daniel K. Akaka
Chairman
Subcommittee on Oversight of Government Management,
the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs
United States Senate

Dear Mr. Chairman:

Radioactive material is used worldwide for legitimate purposes, including medical procedures for treating cancer, purifying blood, or conducting research. Material used for these purposes is typically sealed in a metal capsule such as stainless steel, titanium, or platinum, to prevent its dispersal and is commonly called a sealed source.¹ Some of these sources are highly radioactive, and can be found in medical equipment in U.S. hospitals and medical facilities, which are often open to the public and located in large population centers. The small size and portability of sealed radiological sources make them potentially vulnerable to theft or misuse when not adequately secured.

In the hands of terrorists, these sealed sources could be used to produce a simple and crude but potentially dangerous weapon, known as a dirty bomb, by packaging explosives with the radioactive material for dispersal when the bomb goes off. A dirty bomb detonation would likely result in few deaths, mainly from the explosion, but could create significant social and economic impacts from public panic, decontamination costs, and denial of access to the area in which the detonation took place for extended periods. A 2004 study by the National Defense University noted that the economic impact on a major populated area from a successful dirty bomb attack is likely to equal, and perhaps exceed, that of the September 11, 2001, attacks on New York City and Washington, D.C. The potential impacts of a dirty bomb attack could also produce significant health consequences. In 2002, the Federation of American Scientists concluded that an americium radiological source combined with 1 pound of explosives would require medical supervision and monitoring

¹Such material includes americium-241, cesium-137, and iridium-192.

for the population of an area 10 times larger than the area hit by the initial blast.²

Incidents involving radiological sources can provide a measure of understanding of what could happen in the case of a dirty bomb attack. For example, in 1987, an accident involving an abandoned, or orphaned, teletherapy machine, which is used to treat cancer by focusing a beam of radiation from a highly active radiological source at affected tissue, killed four people and injured many more in the region of Goiania in central Brazil. The device encapsulated about 1,400 curies of cesium-137, which is generally in the form of a powder similar to talc and highly dispersible.³ The accident and its aftermath caused about \$36 million in damages to the region, according to an official from Brazil's Nuclear Energy Commission. In addition, the accident created environmental and medical problems. Specifically, 85 houses were significantly contaminated, and 41 of these had to be evacuated. The decontamination process required the demolition of homes and other buildings and generated 3,500 cubic meters of radioactive waste. Furthermore, over 8,000 persons requested monitoring for contamination in order to obtain certificates stating they were not contaminated.

The Nuclear Regulatory Commission (NRC) regulates the security of radiological sources at commercial facilities, including hospitals and medical facilities. NRC has primary responsibility for licensing, inspecting, regulating, and enforcing the commercial use of radioactive materials. Under NRC regulations, a licensee⁴ is required to secure from unauthorized removal or access licensed materials that are stored in controlled or unrestricted areas.⁵ Furthermore, licensees are required to control and maintain constant surveillance of licensed material that is in a

²Americium-241 is commonly used in smoke detectors.

³A curie is a unit of measurement of radioactivity. In modern nuclear physics, it is precisely defined as the amount of substance in which 37 billion atoms per second undergo radioactive disintegration. In the international system of units, the becquerel is the preferred unit of radioactivity. One curie equals 3.7×10^{10} becquerels.

⁴A licensee is a company, organization, institution, or other entity to which NRC or state agencies have granted a general license or specific license to construct or operate a nuclear facility, or to receive, possess, use, transfer, or dispose of source material, byproduct material, or special nuclear material.

⁵10 C.F.R. § 20.1801.

controlled or unrestricted area and that is not in storage.⁶ However, NRC did not specify in its regulations how licensees were required to implement the specific requirements. After September 11, 2001, NRC reviewed the existing security requirements and determined that increased security of radiological material was necessary. Therefore, NRC issued a security order in 2005 directing those licensees possessing certain types of radiological materials, including those commonly used in hospitals and medical facilities, to implement increased security measures, such as conducting employee background checks.⁷ In 2007, NRC issued an additional security order requiring that individuals requesting unescorted access to radiological material also undergo fingerprinting with verification through the Federal Bureau of Investigation.⁸ In addition, NRC provided licensees with implementation guidance for the two security orders.⁹

On March 14, 2012, we provided preliminary observations on our work concerning radiological source security at U.S. hospitals and medical facilities as part of a testimony before your committee.¹⁰ On March 16, 2012, NRC voted to approve publication of final regulations, which would, among other things, place security measures, fingerprinting, and background check requirements into NRC regulations and replace the existing security orders. NRC is in the process of submitting these final regulations to the Office of Management and Budget for approval and publication, and they will be effective 1 year after publication in the

⁶10 C.F.R. § 20.1802.

⁷Order Imposing Increased Controls. NRC Order EA-05-090. NRC issues security orders to require licensees to implement interim security measures beyond that currently required by NRC regulations and as conditions of licenses.

⁸Order Imposing Fingerprints. NRC Order EA-07-305.

⁹Order Imposing Increased Controls. NRC Order EA-05-090, including Enclosures, Attachments, and Supplemental Questions and Answers. Order Imposing Fingerprints. NRC Order EA-07-305, including Supplemental Questions and Answers.

¹⁰GAO, *Nuclear Nonproliferation: Further Actions Needed by U.S. Agencies to Secure Vulnerable Nuclear and Radiological Materials*, [GAO-12-512T](#) (Washington D.C.: Mar. 14, 2012).

Federal Register.¹¹ The final regulations would add some details to the requirements in the earlier security orders but do not provide a prescriptive framework that would direct hospitals and medical facilities on how to secure their high-risk radiological sources. For example, when the regulations become effective, they will provide hospitals and medical facilities with more specific information on how they must monitor their high-risk radiological sources against tampering and theft, including a requirement that they choose their security measures from a menu of options, such as a monitored intrusion detection system that is linked to an on-site or off-site central monitoring facility or providing direct visual surveillance by approved individuals located within the security zone. However, the pending regulations allow licensees to choose any single option, regardless of the risk posed by the radiological source or the location of the licensee's facility. In addition, the security measures provided in the pending regulations are very similar to the measures outlined in the prior implementation guidance. For the purposes of this report, we are referring to the NRC security orders and implementation guidance, which contain security requirements, as "NRC security controls" or "requirements." For additional information on the current NRC security controls under the NRC security orders and the approved but not yet published final regulations, see appendix II.

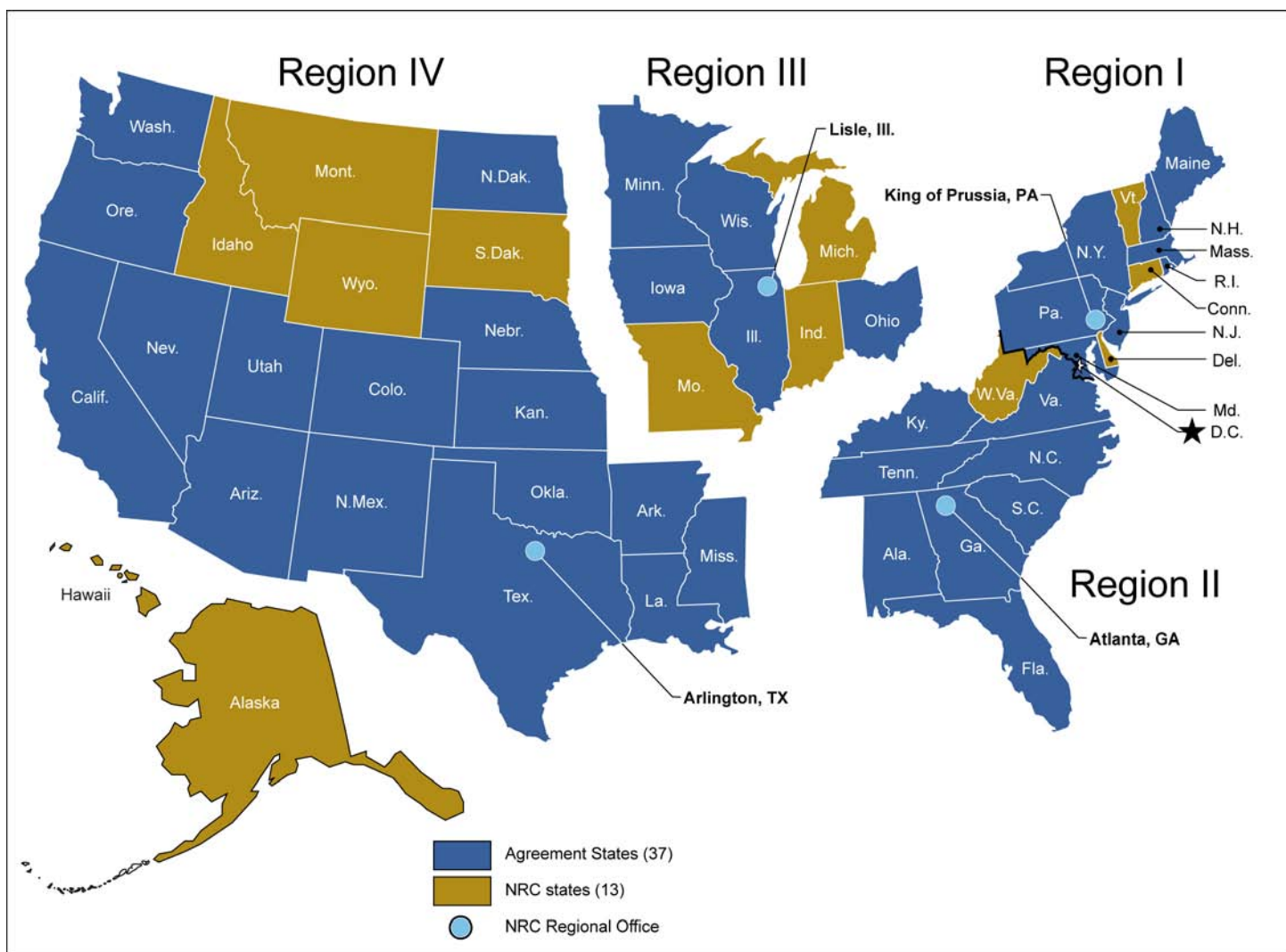
NRC oversees licensees through three regional offices located in Pennsylvania, Illinois, and Texas. NRC has relinquished regulatory authority for licensing and regulating radiological sources to 37 Agreement States,¹² which typically oversee radiological security through their state health or environment departments, and inspect licensees to ensure compliance with state regulations that are generally compatible

¹¹The approval of 10 C.F.R. Part 37 by NRC was announced in an NRC memorandum on March 16, 2012. In the memorandum, NRC staff recommended that the final rule be effective 1 year after publication in the *Federal Register*, with Agreement States required to issue compatible regulations within 3 years of publication. Licensees were not operating under this rule when we conducted our site visits. As of the time of this report, the final regulations have not been published in the *Federal Register*.

¹²Pub. L. No. 83-703 § 274 (1954.) The following are the 37 states that have entered into an agreement with NRC, whereby NRC has relinquished authority, and those states have assumed regulatory authority over certain byproduct, source, and small quantities of special nuclear materials: Alabama, Arizona, Arkansas, California, Colorado, Florida, Georgia, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Nebraska, Nevada, New Jersey, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, and Wisconsin.

with NRC regulations. Figure 1 shows which states are overseen by NRC and which are Agreement States.

Figure 1: Map of NRC Regions and 37 Agreement States



Sources: GAO; Map Resources (map).

Note: Figure 1 depicts NRC's four regions, but only three of these regions oversee licensees with radiological sources. Region I, located in King of Prussia, PA, oversees hospitals and medical facilities within Region II that have radiological sources.

The National Nuclear Security Administration (NNSA), a separately organized agency within the Department of Energy (DOE), established a voluntary program in 2008 as part of its Domestic Material Protection program to provide security upgrades, beyond what NRC requires, to U.S. commercial facilities that contain high-risk radiological materials. The upgrading of hospitals and medical facilities is one component of the Domestic Material Protection program, which also secures high-risk radiological sources in other commercial facilities and sites. NNSA has identified approximately 1,500 U.S. hospitals and medical facilities with high-risk radiological sources that contain approximately 28 million curies of radioactive material and that are candidates for security upgrades.¹³ NNSA also provides training for hospital personnel and local police departments through its Alarm Response Training program at the Y-12 National Security Complex in Oak Ridge, Tennessee. This NNSA-funded training is designed to teach facility personnel and local law enforcement officials how to protect themselves and their communities when responding to alarms indicating the possible theft or sabotage of nuclear or radioactive materials.

Additionally, other federal agencies, such as the Departments of Defense (DOD) and Veterans Affairs (VA), which are NRC licensees, are required to implement their programs to meet all NRC requirements to secure radiological sources at U.S. hospital and medical facilities.

This report responds to your request for a review of radiological source security. For this report, we determined (1) the extent to which NRC's requirements ensure the security of high-risk radiological sources at U.S. hospitals and medical facilities and (2) the progress NNSA has made and the challenges it faces providing security upgrades at U.S. hospitals and medical facilities that contain high-risk radiological sources.

To conduct this work, we reviewed relevant laws, regulations, and guidance for overseeing radiological sources. We interviewed agency officials at NNSA, NRC, DOD, VA, and the Departments of Homeland Security (DHS), and Justice (DOJ). We also interviewed experts in the

¹³High-risk radiological sources have been identified by international organizations as the sources that pose the greatest risk to human health and safety, and should be afforded a greater level of security. NNSA has determined the buildings in which these radiological sources are located. For the purposes of this report, we are using the term "facilities" rather than "buildings" for the purpose of consistency.

field of nuclear security, state government officials in selected states, and safety and security personnel at hospitals to obtain their views on how radiological sources are secured at U.S. hospitals and medical facilities.¹⁴ To examine how NRC's requirements affect the security of high-risk radiological sources at U.S. hospitals and medical facilities, we collected information and interviewed agency officials responsible for overseeing and securing sources at NRC, NNSA, VA, DOD, DHS, and DOJ. We also gathered information from Agreement States and NRC regions by collecting information and interviewing officials at 20 selected Agreement States and the three NRC regional offices with responsibility for overseeing high-risk radiological sources.¹⁵ To learn how NRC requirements are implemented at the facilities, we visited 26 hospitals and medical facilities in California, Maryland, New York, Pennsylvania, Tennessee, Texas, Virginia, and Washington, D.C. We selected these hospitals and medical facilities on the basis of geographic dispersion, the amount of curies contained in their radiological sources, and types of radiological devices. The facility information is not generalizable to all hospitals or medical facilities but provides illustrative examples. We also visited local law enforcement agencies in California, New York, and Washington, D.C. To evaluate the extent to which NNSA has enhanced the security of high-risk radiological sources at U.S. hospitals and medical facilities and the challenges they face, we analyzed information from and interviewed NNSA officials about their Domestic Material Protection program, which partners with hospitals and medical facilities to provide voluntary security upgrades to facilities with high-risk radiological sources. We also visited facilities that received NNSA upgrades and security assessments in California, New York, Pennsylvania, Tennessee, Texas, Virginia, and Washington, D.C. These facilities were selected to provide us with a cross section of hospitals and medical facilities that had completed security upgrades, were in the process of completing upgrades, or had volunteered for the program and were negotiating with

¹⁴Experts were selected based on their previous work in radiological source security, both within the United States and internationally.

¹⁵We spoke with officials about how Agreement States implement the NRC security controls from the following 20 of the 37 Agreement States: Alabama, Arizona, Arkansas, California, Colorado, Florida, Kentucky, Maryland, Massachusetts, Mississippi, New Mexico, New York, North Carolina, Pennsylvania, Rhode Island, Tennessee, Texas, Virginia, Washington, and Wisconsin. We also spoke to officials in NRC Regions I, III, and IV. We selected the Agreement State and NRC Regional Office officials based on their experience with securing high-risk radiological sources across the United States.

NNSA about the scope of the upgrades. To determine the costs of these security upgrades, we obtained cost data from NNSA and interviewed the agency officials who oversee the program. To assess the reliability of these data, we discussed their reliability with knowledgeable NNSA officials and questioned them about the system's internal controls to verify the accuracy and completeness of the data. We found the data sufficiently reliable for our reporting purposes. Appendix I presents a more detailed description of our scope and methodology.

We conducted this performance audit from April 2011 to September 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Radiological sources are used throughout the world for peaceful purposes. Until the 1950s, only naturally occurring radioactive materials, such as radium-226, were available to be used in radiological sources. Since then, sources containing radiological material produced artificially in nuclear reactors and accelerators have become widely available, including cesium-137, cobalt-60, iridium-192, and strontium-90, which are used to treat cancer through radiotherapy and cesium-137, which is also used to treat blood. See figure 2, which shows an example of an americium-241 sealed radiological source. Sealed sources vary in size from the size of a pencil eraser to rods up to several inches in length.

Figure 2: Example of a Radioactive Sealed Source That Contains Americium-241



Source: DOE.

Radiological material can be found in various forms, such as metals or powders, and is measured by its level of activity. The greater the activity level—measured in curies—the more radiation emitted, which increases the potential risk to public health and safety if improperly used or controlled. The intensity of radiological materials decays over time at various rates. The term “half-life” is used to indicate the period during which the radioactivity decreases by half as a result of decay. In general, the shorter the half-life and the larger the mass, the more radiation will be emitted within a particular period.

According to the International Atomic Energy Agency (IAEA),¹⁶ the level of protection provided by users of the radiological material should be commensurate with the safety and security risks that it presents if improperly used. For example, radiological materials used for certain diagnostic purposes, such as diagnostic imaging, have low levels of activity and do not present a significant safety or security risk. However, high-risk sealed radiological sources that contain cobalt-60, cesium-137 or iridium-192, could pose a greater threat to the public and the environment and could also pose a potentially more significant security risk, particularly if acquired by terrorists to produce a dirty bomb.

NRC regulates medical, industrial, and research uses of radiological materials through a combination of activities, including regulatory requirements; licensing; and safety and security oversight, including inspection and enforcement. NRC issues licenses for the possession and use of this material in items such as sealed sources.¹⁷ Each licensee designates one or more employees, often typically a Radiation Safety

¹⁶IAEA is an independent international organization based in Vienna, Austria, that is affiliated with the United Nations and has the dual mission of promoting the peaceful uses of nuclear energy and verifying that nuclear materials intended for peaceful purposes are not diverted to military purposes.

¹⁷Two types of licenses are associated with the use of radioactive materials—general licenses and specific licenses. General licenses are associated with products that contain some radioactive material, such as fixed gauges or exit signs, and the owners of these products do not have to apply to NRC or an Agreement State for a license. A company seeking radiological material for uses that do not qualify for a general license must apply to NRC or, if it conducts business in an Agreement State, to the appropriate state office for a specific license. Specific licenses include those of “limited scope,” in which radioactive materials will be used by a defined number of authorized users, and those of “broad scope,” for facilities that have experience successfully operating under a specific license of limited scope.

Officer (RSO), to oversee compliance with applicable NRC and Agreement State regulations, including security controls.

NRC has stated that nuclear and radiological materials are critical and beneficial components of global medical, industrial, and academic efforts. However, the possibility that these materials could be used by terrorists is a national security concern. As a result, NRC tracks the number of hospital and medical facility licensees with radionuclides of concern through its National Source Tracking System.¹⁸ This database provides a “cradle-to-grave” account of the origins of each radiological source (manufacture, remanufacturing, or import) and records who used it and eventually disposed of, or exported it. NNSA coordinates with NRC to receive these updated data and has further enhanced the data for its purposes, including identifying which radioactive materials are associated with which licenses and what sources are located in which facilities.

NRC Requirements and Implementation by Licensees Do Not Ensure the Security of High-Risk Radiological Sources

At the 26 selected hospitals and medical facilities we visited, NRC’s requirements did not consistently ensure the security of high-risk radiological sources. One reason for this is that the requirements, which are contained in NRC security controls (i.e., the two security orders and implementation guidance) are broadly written and do not prescribe specific measures that licensees must take to secure their equipment containing high-risk radiological sources. Some of the NRC-licensed hospitals and medical facilities we visited are more at risk than others to sabotage and theft because some hospitals developed better security for protecting their radiological sources than others. Licensees have implemented these broad requirements in various ways, leaving some hospitals’ radiological sources more vulnerable than others. In addition, some inspectors said that the NRC-required training is not sufficient, and personnel at hospital and medical facilities are not required to have security training, although they implement NRC requirements at their sites. NRC reviews of Agreement States also found that some Agreement States do not have sufficient staffing and resources to enforce NRC security controls.

¹⁸Radionuclides of concern is the term NRC uses to identify types of radiological material that require additional security when total activity crosses thresholds due to the type or quantity of the source.

NRC's Security Requirements Governing Radioactive Material Are Non prescriptive

NRC's requirements direct licensees possessing high-risk radiological material contained in medical equipment to implement increased security measures. However, these requirements are broadly written and do not prescribe the specific steps hospitals and medical facilities must take to secure the material. Rather, the security controls and their requirements provide a general framework for what constitutes adequate security practices. The officials said that the key elements of the framework include: (1) limiting access to only approved individuals through the use of background checks that include fingerprinting; (2) enhancing physical barriers and intrusion detection systems; (3) coordinating with local law enforcement to respond to an actual or attempted theft, sabotage, or diversion of radiological material; (4) promptly notifying authorities of incidents; and (5) monitoring shipments of radiological material during transit. According to NRC officials, the intent of the security controls is to develop a combination of people, procedures, and equipment that will delay and detect an intruder and initiate a response to the intrusion—not to provide absolute security from theft or unauthorized access. The security controls provide minimum requirements that must be met to ensure adequate security, and licensees may go beyond the minimum requirements.

NRC officials told us that they have adopted a risk-based approach to security, in which the level of security should be commensurate with the type and amount of sources they are attempting to protect. In addition, NRC officials said that they take facility costs into consideration when issuing new security requirements. The risk-based approach reflects the agency's concerns regarding the potential adverse financial effect that additional security measures could have on private medical facilities throughout the United States. As a result, the security controls issued by NRC are intentionally broad to allow licensees flexibility when implementing security upgrades. However, according to NRC officials, NRC requirements relating to the adequate protection of public health and safety do not consider costs. The officials state that this approach aligns with Executive Order 12866, which directs Executive Branch agencies to tailor their regulations to impose the least burden on society, including individuals, businesses of differing sizes, and other entities (including small communities and governmental entities), consistent with obtaining the regulatory objectives, taking into account, among other things, and to the extent practicable, the costs of cumulative regulations. However, the Executive Order requirements in pertinent part do not apply to the NRC, but NRC follows many of the provisions voluntarily. In late April 2012, NRC released a document that stated, among other things, that its security program is a multilayered, non prescriptive framework that allows

licensees to develop security programs specifically tailored to their facilities. NRC officials told us that due to diverse economic conditions, facility type, layout, and operations of hospital and medical facilities, a “one size fits all” approach to radiological source security is neither practical nor desirable. The officials said that the ability to tailor security to a facility’s needs and resources is particularly important for commercial facilities with limited resources. For example, personnel from one smaller medical facility we visited told us that implementing specific security requirements—such as cameras and other surveillance equipment—could jeopardize their continued operations because of the costs associated with the installation and maintenance of this equipment.

NRC’s implementation guidance, which supplements the security orders, provides examples of how hospitals and medical facilities can secure their high-risk radiological material and meet security requirements. In their implementation guidance, NRC provides that facilities may meet the security requirements by, for example, limiting the distribution of keys, key cards, or combinations to doors and gates to approved individuals; activating locked doors and gates by using remote surveillance; using a card reader and electronic locking devices at control points; and having a person approved for unescorted access conduct constant surveillance of the devices containing the radiological material.

However, ultimate responsibility for implementing NRC’s security controls is left to the discretion of the hospital and medical facility personnel that possess the materials. The controls do not prescribe the specific measures that licensees must take to secure their sources, such as the use of cameras, alarms, and other physical security measures. The licensee determines, for example, if security cameras are necessary or what types of locks or alarms, if any, are needed to secure doors or windows. For some locations we visited that are staffed 24 hours a day, 7 days a week, such as blood banks, requirements for access control can be met when the room where the medical device containing radiological material is located is continuously staffed by an individual or individuals who are determined to be trustworthy and reliable. As long as the room is staffed at all times, the facility is not required to have any additional physical security, such as cameras or motion detection equipment.

NRC’s security controls require hospital and medical facility personnel to conduct background checks to determine the trustworthiness and

reliability of individuals requesting unescorted access to radiological material.¹⁹ NRC officials told us that background checks are important for protecting against an “insider threat,” in which someone with access to the radiological material might try to remove, tamper with, or sabotage the source. NRC’s implementation guidance states that the commission’s requirements are not intended to stop determined adversaries intent on malevolent action from gaining access to the radioactive material. Rather, these requirements are designed to provide reasonable assurance that individuals with unescorted access to the radioactive material are trustworthy and reliable and that facilities have a reliable means to rapidly identify events that are potentially malevolent and have a process for prompt police response. Furthermore, hospital and medical facility officials are responsible for appointing a trustworthiness and reliability official (T&R official), who is to determine which employees will be granted unescorted access to the device containing radioactive material. The T&R officials at the 26 hospitals and medical facilities we visited were typically RSOs, security officials, or officials from the human resources department. When granting unescorted access for individuals employed less than 3 years, NRC also requires hospitals and medical facilities to, at a minimum, verify employment history, education, and personal references. For individuals employed for longer than 3 years, facilities are to determine trustworthiness and reliability, at a minimum, by reviewing the employee’s employment history with the facility.

Officials at 5 of the 26 hospitals and medical facilities we visited told us they face challenges in determining which individuals are suitable for a trustworthiness and reliability certification. For example, two of these five officials said that the current background examination process places too much emphasis on the judgment of hospital personnel. Performing background checks on foreign nationals is also particularly challenging. Officials at 6 of the 26 hospitals and medical facilities we visited agreed, citing, for example, the difficulty in acquiring relevant background information from different countries, the inability to corroborate written documentation, and language barriers. Administrators at 2 of these 6 hospitals also told us that a more centralized background examination process with uniform criteria and standards should replace the current system, which varies from facility to facility.

¹⁹Pub. L. No. 109-48 § 652 (2005) amended the Atomic Energy Act to require fingerprinting and criminal history checks for any individual who is permitted unescorted access.

Some Medical Facilities Licensed by NRC Are More Vulnerable Than Others to Potential Sabotage and Theft Because of Security Weaknesses

The 26 hospitals and medical facilities we visited in seven states and Washington, D.C., have implemented NRC's security controls in a variety of ways that could leave some facilities' radiological sources more vulnerable than others to possible tampering, sabotage, or outright theft because, on their own initiative, some facilities have decided to implement more stringent security measures than others.

Law enforcement personnel from states with significant amounts of high-risk radioactive material told us that NRC's security controls have an inherent weakness: they do not specify what the facility is protecting against and are not linked to a design basis threat. According to IAEA, a design basis threat includes the attributes and characteristics of a potential insider and/or external adversaries, who might attempt unauthorized removal or sabotage, against which a physical protection system is designed and evaluated. NRC officials noted that, according to IAEA's Nuclear Security Series Implementation Guide No. 11, "Security of Radioactive Sources," the design and evaluation of a security system should take into account the current national threat assessment and may include the development and application of a design basis threat, although it is not required.

Typically, a design basis threat characterizes the elements of a potential attack, including the number of attackers, their training, and the weapons and tactics they are capable of employing. Instead, NRC relies solely on the amount of curies under the control of a hospital or medical facility when determining if the facility is subject to increased security controls. According to NRC, it would not be feasible to require a design basis threat analysis for U.S. hospitals and medical facilities because of the varied nature of the facilities and the additional resources required to conduct an analysis for individual facilities. NNSA also does not use a design basis threat for its security assessments of hospitals and medical facilities but does employ a threat scenario (known as potential adversary capability) as the basis for its recommendations for security enhancements. NNSA defines Potential Adversary Capabilities as the method for documenting a realistic threat level that the security upgrades must enhance protection against. At VA, which is overseen by NRC under

a Master Materials License (MML),²⁰ the official responsible for radiological security told us that VA initially developed a generic threat scenario for use at its facilities with high-risk radiological materials because NRC did not provide a design basis threat as part of its security controls. Later, VA coordinated closely with NNSA to complete security assessments and install security upgrades at the VA facilities with high risk sources. The assessments were completed from 2009 through 2011, with installation of the agreed upon security upgrades currently ongoing. VA facilities have also participated in the NNSA Alarm Response training program.

All of the 26 medical facilities we visited have implemented NRC's security controls and undergone inspections by either NRC or Agreement State inspectors. At some facilities, the implementation of the controls resulted in significant security upgrades, such as the addition of surveillance cameras, upgrades to locks on doors, and alarms. NRC stated that, although hospitals are open to the public, the specific location housing a radiological source generally is not. These sources are shielded inside medical devices that can weigh thousands of pounds, which make it difficult to remove or tamper with the radiological material, according to NRC.

Notwithstanding NRC's views, we observed potential security weaknesses in several facilities we visited, such as the following:

- At a hospital in one state, two cesium-137 research irradiators (i.e., used for medical or biological research), that contain approximately 2,000 curies and 6,000 curies, respectively, are housed in the basement of a building that is open to the public. The hallway leading to the irradiator room has a camera, but it is pointed away from the room. The door to the room is opened by a swipe card lock, and there are no cameras or other security measures inside the room. We observed that one of the irradiators was sitting on a wheeled pallet. When we asked the RSO if he had considered removing the wheels,

²⁰NRC issues licenses to VA facilities under an MML. An MML is a material (byproduct, source, and/or special nuclear material) license issued to a federal organization, authorizing use of material at multiple sites. The MML authorizes the licensee to issue permits for the possession and use of licensed material under the license and ties the licensee to a framework for oversight and internal licensee inspection of the MML. A master materials licensee remains an NRC licensee and MML permittees are required to meet NRC regulatory requirements.

he said no. Furthermore, we observed that the irradiator room is located in close proximity to an external loading dock and that the cameras along the corridor to the loading dock are displayed on a single monitor, making it difficult for someone monitoring the corridor to interpret what activity is occurring. This facility had passed its most recent NRC security inspection, according to a hospital official, because access to the room where the irradiators were located was restricted through use of a swipe card. However, this facility could be vulnerable because of the limited security we observed and the mobility of one of the irradiators.

- At a hospital in a major U.S. city, we observed that the interior door to the hospital blood bank, which had a cesium-137 blood irradiator of approximately 1,500 curies,²¹ had the combination to the lock written on the door frame. The door is in a busy hallway with heavy traffic, and the security administrator for the hospital said that he often walks around erasing door combinations that are written next to the locks. According to NRC officials, a single lock is not necessarily a security weakness; however, failure to control the combination and restrict access to only trustworthy and reliable individuals is a clear violation of NRC requirements. Figure 3 shows the combination written on the door frame to the blood bank.

²¹Irradiating blood keeps white cells in the blood from attacking host tissue after a transfusion.

Figure 3: Combination to Lock on Door Frame Outside Blood Bank



Source: GAO.

- At a blood center in a third state we visited, we observed a cesium-137 blood irradiator of approximately 1,400 curies in a room that was secured by a conventional key lock. The irradiator was located in the

middle of the room and not secured to the floor. The room had an exterior wall with a bank of unalarmed and unsecured windows that looked out onto a publically accessible loading dock. The blood center officials said that, while they met NRC's security controls, they acknowledged that the center is highly vulnerable to theft or sabotage of their radiological sources. According to NRC officials, an irradiator sitting in the middle of the floor that is not bolted down is not necessarily vulnerable. Figure 4 shows the irradiator that is not bolted to the floor and the bank of unsecured windows looking out onto the loading dock.

Figure 4: Irradiator and Bank of Unsecured Windows Looking Out onto Loading Dock



Source: GAO.

-
- The RSO at a large university hospital told us that he did not know the exact number of people with unescorted access to the hospital's radiological sources, although he said that there were at least 500. The hospital's current data system does not allow for entering records for more than 500 individuals. In the past, he said, the hospital had as many as 800 people with unescorted access to sources. In contrast, at a major medical research facility on a military installation we visited, access was limited to 4 safety and security personnel.

Some NRC and Agreement State Inspectors and Hospital and Medical Facilities Lack Training and Resources to Enforce NRC Requirements

NRC and Agreement State inspectors and hospital and medical facility personnel we interviewed said that the NRC training has not prepared them to adequately enforce NRC requirements. Furthermore, personnel at the facilities said that they may not have the resources they need to implement the security controls.

NRC and Agreement State Inspectors May Not Be Adequately Trained to Provide Effective Security Oversight

Some inspectors from NRC and Agreement States said that they have not received adequate training from NRC on securing high-risk material at hospitals and medical facilities. NRC requires that NRC and Agreement State inspectors take training for implementing the security controls. NRC has developed and provides a 5-day security training course for NRC and Agreement State inspectors on how to implement the security controls. The course takes place at DOE national laboratories, with recent training occurring at Sandia National Laboratory in New Mexico. It includes 17 modules providing information on how to protect against malicious uses of radioactive materials, such as the introduction to physical protection, target identification, intrusion detection, security lighting, access control systems, barriers, locking systems, and response forces. The course also covers NRC security controls associated with the increased security measures. However, even with this training, 6 of the 48 inspectors we spoke with who cover both NRC regions and Agreement States told us that they do not feel comfortable conducting security inspections at hospitals and medical facilities. According to the inspectors, NRC's training course provides an introduction to security practices for those with limited security experience and trains inspectors generally in how to conduct security inspections. The inspectors typically have educational backgrounds in radiation safety or health physics rather than security. The inspectors said that not having security experience has made it difficult for them to transition to conducting security inspections. Examples are as follows:

Hospital and Medical Facility
Personnel Do Not Have the
Training to Implement NRC's
Security Controls

- An Agreement State inspector told us that he attended NRC's training program, but he did not believe that it sufficiently prepared him to be a security expert and make the kinds of judgments required to determine whether licensees have adequate security.
- Inspectors from another Agreement State told us that the course did not cover certain topics that they thought were essential to radiological security, such as the use of radiation detectors. They also said that they were placed in the awkward situation of having to enforce NRC's security orders, which they did not believe they were fully qualified to interpret.
- Another Agreement State inspector from a third state we visited told us that he was not qualified to do security inspections. However, he said that he was doing the best he could to interpret the NRC security controls and help the licensees implement the requirements.
- An NRC inspector also said that security inspections were particularly difficult for him because he is trained as a physicist. He said that the security controls were confusing and that he did not understand the nuances of security.

NRC's security controls require hospitals and medical facilities to develop a program for assessing and responding to unauthorized access, including detecting an unauthorized intrusion, assessing the situation, and calling for a response from the local law enforcement agency of an actual or attempted theft of the high-risk radiological materials or the device itself. However, none of the personnel who are responsible for implementing the security controls for high-risk radiological sources at the 26 hospital and medical facilities we visited has been trained in how to implement NRC's security controls. In addition, 15 officials at the 26 hospitals and medical facilities told us that they have backgrounds in radiological safety and facilities management and have limited security experience, making them responsible for security with limited previous experience to draw from. We found the following examples:

- At one hospital, the RSO said that when the security controls were instituted in 2005, his new responsibilities included ensuring the security of a cobalt-60 gamma knife of approximately 2,600 curies, which is used to treat cancer patients, and a cesium-137 blood irradiator of about 2,400 curies. He told us that he was not comfortable with his security role because he was trained as a health physicist.

-
- One facility manager who oversees the security for an approximately 1,700 curie cesium-137 blood irradiator at a blood bank told us that he has a background in construction, not security. He said that it would have been helpful if NRC's controls were more prescriptive, including better guidance, so that he would be in a better position to determine what security would be most effective.

NRC requires medical facility officials to demonstrate radiation safety expertise through a combination of education and work experience to be eligible to become an RSO. However, the security controls do not require that RSOs or other designated security officials have security experience or that they take NRC security training. For example, NRC regulations state that individuals may meet the eligibility requirements for becoming an RSO by completing a master's degree or doctoral degree in health physics or a related field, combined with 2 years of full-time experience under the supervision of a board-certified medical physicist.²² In addition, NRC's new regulations, when finalized, will require that officials at hospitals and medical facilities provide training on their security program and procedures to personnel involved in securing high-risk radiological material. However, the regulations do not require that the RSO, who is typically responsible for providing the training, has any formal security education or work experience, although the RSO is responsible for the security of radiological sources. Without training and adequate guidance, medical facility officials, including RSOs, who may be responsible for implementing NRC's security controls, may not have adequate knowledge of securing equipment containing high-risk radiological sources.

Some Agreement States Do Not Have Sufficient Staffing and Resources to Enforce Security Controls

NRC's recent reviews of Agreement States' inspection programs showed a lack of adequate staff, resources, and security training in two states.²³ In its review of one of the state's inspection programs, NRC reported that the program experienced significant turnover and that inspectors did not have an adequate understanding of the security controls. According to an official in this state, high staff turnover and the resulting lack of security experience affected the quality of the state's oversight. In addition, staff

²²10 C.F.R. § 35.50.

²³NRC's Integrated Materials Performance Evaluation Program reviews Agreement State programs to ensure that they meet NRC's standards. Since 2006, NRC has conducted 41 reviews that contained reports on states' performance in the inspection and licensing under NRC's security controls.

turnover issues have kept inspectors from receiving needed on-the-job training or mentoring from experienced inspectors. As a result, inspectors have difficulty assessing whether licensees comply with NRC security controls. According to NRC's review of the state program, the state inspectors took steps to incorporate interviews with appropriate personnel and performance observations into their inspection activities. However, inspectors often did not adequately follow up on potential items of non-compliance that were observed during the performance reviews. NRC's review noted that the state inspectors did not have sufficient familiarity with NRC's security controls and therefore had difficulty assessing licensee compliance with the requirements. In one case, the inspector did not identify or understand the security significance of an item of noncompliance. In addition, during a final meeting with the facility personnel responsible for managing the license, the inspector could not clearly articulate the applicable requirements and was unable to explain to the licensee what actions could be taken to correct the identified deficiencies.

NRC reported that Agreement State inspectors completed some level of preparation, such as reviewing NRC's security controls, prior to their inspections but, in some cases, their preparation was inadequate. In addition, NRC officials stated that, in accompanying Agreement State inspectors, they identified problems with the completeness of their reviews, technical quality, consistency, and attention to health and safety/security. NRC noted that the deficiencies were indicative of a programmatic and chronic problem rather than an isolated occurrence or a periodic decline in performance.

In its review of another Agreement State's program, NRC stated that new inspectors would have benefitted from additional training on NRC's security controls. An Agreement State inspector told NRC's review team that he did not understand the meaning of some of the documents he was reviewing. Another Agreement State inspector stated that he was authorized to inspect a radiological device independently—without being accompanied by a more experienced inspector—before he was ready to do so. In addition, some Agreement State inspectors told NRC's review team that they sometimes performed inspections without the added benefit of having attended a training class for the type of inspection being performed, primarily because they were unable to get into the classes. One state program manager, who acts as the primary trainer for a state inspection program, acknowledged to the NRC review team that because of her workload she often has to limit the number of training classes offered.

NNSA Completed Security Upgrades in More Than 300 Medical Facilities, but Some Hospitals Do Not Participate in the Voluntary Program

As of April 2012, NNSA had completed security upgrades at 321, or one-fifth, of the 1,503 U.S. hospital and medical facilities it had identified as having high-risk radiological material but does not expect to complete all such upgrades until 2025. In addition, the program's impact is constrained because: (1) it is voluntary, (2) hospitals and medical facilities will have to maintain the upgrades beyond NNSA's 3- to 5-year warranty period, and (3) the program does not require facilities to sustain the upgrades.

NNSA Has Made Progress in Securing Radioactive Sources, but Does Not Expect to Complete All 1,500 Medical Buildings Until 2025

NNSA's Domestic Material Protection program is designed to raise the security at U.S. facilities with high-risk radiological material, including hospitals and medical facilities, to a level that is above NRC and the Agreement State's regulatory requirements. NNSA's voluntary program provides these U.S. hospitals and medical facilities with security assessments, but the agency does not share these assessments with NRC and Agreement State inspectors. According to NNSA officials, the agency does not share the assessments because of its concern that hospitals and medical facilities, which are voluntarily cooperating with NNSA, would not provide complete and candid information to NNSA if it shared the assessments with NRC and Agreement State's regulatory inspection agencies. After completing the assessments, NNSA installs security upgrades, such as remote monitoring systems, biometric access controls, and security cameras, to secure the devices and facilities that contain high-risk radiological sources. NNSA pays the cost for all security upgrades, but hospitals and medical facilities are responsible for maintaining the security systems after a 3- to-5-year warranty period expires. According to NNSA officials, during the warranty period, sustainability costs for the upgrades at each hospital average \$40,000 per facility per year, including equipment warranty and maintenance costs, as well as the costs associated with labor and site visits to ensure that the hospitals are properly operating the NNSA upgrades. The NNSA officials estimate that when the hospitals are ready to assume full responsibility for the security upgrades at their facilities, the sustainability costs assumed by the hospitals are approximately \$10,000 per facility per year.

Of the 1,502 U.S. medical facilities NNSA has identified that contain high-risk radiological sources, the agency has provided security upgrades to 321, or about 21 percent of them. The 1,502 facilities cumulatively contain about 28 million curies of radioactive material, according to NNSA's

estimate.²⁴ According to NNSA officials, as of March 2012, the Domestic Material Protection program had spent approximately \$105 million to provide security upgrades to radiological sources at the 321 facilities. NNSA plans to complete security upgrades at all 1,502 medical facilities it has identified as high risk by 2025, at a projected cost of \$608 million. NNSA officials also told us that they estimate the average cost to upgrade a medical facility has been \$317,800.²⁵ NNSA officials told us that their goal is universal participation in their program by all licensees holding high-risk radiological sources.

NNSA provided a further breakdown of the approximately \$105 million that was spent as of March 1, 2012. As table 1 shows, the majority of program expenditures were to complete security assessments and equipment upgrades—such as cameras, motion detection devices, and alarms—at U.S. hospitals and medical facilities. NNSA spent approximately \$99 million, or 95 percent of its total program costs, on equipment, labor, and travel costs associated with the security assessments and upgrades—primarily carried out by personnel from Sandia National Laboratory, Pacific Northwest National Laboratory, and private-sector security vendors. The program spent an additional \$975,800, or 1 percent of its total costs, on designing and testing equipment used for security upgrades. The remaining \$4.3 million, or 4.1 percent of NNSA’s total costs, was spent on laboratory overhead charges and contract fees.

²⁴According to NNSA officials, this estimate reflects the amount of curies for the licensed maximum for each device containing radiological material. It does not reflect what the actual amount of curies may be, because curie levels diminish over time as the radioactive material decays or as the device is utilized. In addition, the total curie amount includes 11 panoramic irradiators with cobalt-60 sources that can range up to 10 million curies per device. We plan to include a review of the panoramic irradiators in a follow-on engagement.

²⁵According to NNSA officials, training costs were excluded from the estimate.

Table 1: Breakdown of NNSA Total Costs for Domestic Material Protection Program, as of February 29, 2012

Dollars in thousands

Performer	Laboratory labor ^b	Laboratory travel ^c	Laboratory equipment ^d	Private sector/non-laboratory ^e	Laboratory contract fees ^f	Total medical building costs	Percentage of total
LLNL	\$385.5	\$77.6	\$2.0	\$0.4	\$0.0	\$465.6	0.4%
NS-E ^a	\$0.0	\$0.0	\$0.0	\$132.4	\$0.0	\$132.4	0.1
ORNL	\$336.4	\$26.0	\$0.0	\$0.0	\$0.0	\$362.4	0.3
PNNL	\$9,022.4	\$1,125.4	\$0.0	\$53,850.1	\$1,791.9	\$65,789.9	62.9
SNL	\$11,339.4	\$1,139.8	\$967.1	\$21,134.5	\$2,062.1	\$36,642.9	35.0
Y-12	\$483.0	\$218.8	\$6.7	\$19.6	\$438.9	\$1,166.9	1.1
Total	\$21,566.7	\$2,587.7	\$975.8	\$75,137.0	\$4,293.0	\$104,560.1	100.0%
Percentage of total	20.6%	2.5%	0.9%	71.9%	4.1%	100.0%	

Legend

LLNL = Lawrence Livermore National Laboratory

NS-E = National Nuclear Security Administration (NNSA) Albuquerque Complex

ORNL = Oak Ridge National Laboratory

PNNL = Pacific Northwest National Laboratory

SNL = Sandia National Laboratory

Y-12 = Y-12 National Security Complex

Source: NNSA.

^aThe Albuquerque Complex provides procurement, business, technical, financial, legal, and management advice and services to support the NNSA mission.

^bIncludes all time spent completing a project, including assessments, upgrade recommendations, travel time, and project reports. Also includes some indirect time such as project management and support, but typically does not include training.

^cIncludes airfare, lodging, and per diem for laboratory personnel.

^dIncludes all equipment and material purchased by DOE laboratories for use, testing, or design of security upgrades. The equipment is not installed at hospitals or medical facilities.

^eIncludes all contract costs with the private sector, including the equipment, labor, and travel costs for participating hospitals and medical facilities and the private-sector security vendors to install the security upgrades.

^fIncludes all laboratory overhead charges and fees applied to contract costs with private-sector security vendors.

Of the 26 hospitals and medical facilities that we visited in seven states and the District of Columbia, 13 had received NNSA upgrades, and 3 were in the process of receiving upgrades. Officials from 11 of the 16 hospitals and medical facilities told us that the NNSA program enhanced the security of their facilities. We observed a number of security upgrades at these facilities, including remote monitoring systems, surveillance cameras, enhanced security doors, iris scanners, motion detectors, and tamper alarms. In addition, NNSA officials told us that as part of the

program they fund the installation of in-device delay kits. These kits are installed in the interior of medical equipment to make it more difficult to remove or tamper with radiological material contained within the equipment. NNSA officials told us that they currently contract with three companies to install the kits in irradiators and have partnered with another company to upgrade the security of new gamma knives. Figures 5, 6, 7, and 8 provide examples of the different NNSA upgrades.

Figure 5: NNSA-Installed Remote Monitoring System



Source: GAO.

Figure 6: NNSA-Installed Iris Scan with Hospital Card Reader



Source: GAO.

Figure 7: NNSA-Installed Security Camera



Source: GAO.

Figure 8: Irradiator with NNSA-Installed Tamper Alarm around Middle of Device



Source: GAO.

Some Facilities Declined NNSA Security Upgrades and Sustainability Is Uncertain

The voluntary nature of the NNSA program allows hospitals and medical facilities to decline the upgrades, even though NNSA assumes all up-front capital costs. Most hospitals and medical facilities we visited were amenable to participating in the program, but NNSA officials told us that, as of July 2012, 14 facilities have declined to participate in the voluntary security upgrade program. These 14 facilities contain over 41,000 curies of high-risk radiological material. According to NNSA officials, 9 of these facilities declined to participate because facility management decided not to accept any NNSA assistance; 3 were unwilling to accept the full suite of NNSA security upgrades; and 2 were either facing bankruptcy or were planning to have their radiological sources removed. Four of the 14 facilities are located in large urban areas that NNSA officials consider high risk.

We met with officials from one hospital and one medical facility that declined the NNSA upgrades. Both facilities were located in densely populated urban areas. Specifically, we found the following:

- According to police department officials in a major U.S. city, one hospital with a blood irradiator of approximately 1,700 curies has declined the NNSA upgrades, even though the police department considers it to be a high-risk facility. The hospital officials told us that they decided not to implement the NNSA upgrades because of concerns about maintenance costs associated with the security equipment after the 3- to 5-year NNSA-funded warranty period expired. The RSO said that the security that the hospital has in place is adequate. Furthermore, the RSO told us that the hospital is under serious budget pressure that makes it difficult to justify spending more money to sustain equipment for protecting their radiological sources.
- Staff at a blood bank with a cesium-137 blood irradiator of approximately 1,400 curies told us that NNSA was prepared to upgrade the facility's security but that the blood bank decided not to participate. The blood bank officials said that senior management wanted to wait until the blood bank moved to a new location, which it planned to do within the next 3 years. However, we observed that the blood irradiator was vulnerable to theft or tampering and discussed these vulnerabilities with the blood bank officials, who agreed that their device was vulnerable. In February 2012, we contacted NNSA officials about this matter. As a result, the facility decided to volunteer for the NNSA program, and NNSA and national laboratory officials met with facility personnel and developed a plan to increase the security of the irradiator by October 2012.

NNSA requires that hospitals and medical facilities sign a sustainability statement, outlining responsibility for the security of high-risk radiological material and stating that they will assume full responsibility for the operation, testing, and maintenance of the security system after the NNSA-funded warranty period expires. However, the agency does not require that hospitals and medical facilities maintain the installed security upgrades beyond the 3- to 5-year warranty period. Nine hospital and law enforcement officials in three states we visited told us that not having such a requirement to sustain NNSA's upgrades limits the program's impact. NNSA officials told us that before they agree to implement the security upgrades, they attempt to determine if a site is committed to sustaining them. NNSA requires that hospital and medical facility officials sign the sustainability statement after completion of the design, but prior to the installation of the security upgrades. However, the NNSA officials told us that the sustainability statement is not legally binding.

NNSA Generally Targets Security Upgrades to States with Significant Amounts of High-Risk Radiological Material

According to our review of NNSA documents and interviews with NNSA officials, NNSA is, for the most part, funding security upgrades in states that have the most high-risk radiological material at hospitals and medical facilities. NNSA has developed a prioritization methodology that ranks different facilities and is designed to assign resources according to the relative risk of the radiological material and the expected risk reduction resulting from the planned security activity. NNSA's prioritization criteria include four factors: (1) attractiveness level of the radiological material,²⁶ (2) site security conditions, (3) threat environment, and (4) location or proximity to a target. In addition, NNSA officials told us that when ranking facilities for upgrades, they consider whether the facility has requested or volunteered for a security assessment under the program, if there are multiple high-risk sources in the same facility, and if NNSA can gain access to a number of sites through a partnership with other federal agencies and organizations such as the Department of Agriculture, the National Institutes of Health, and the American Red Cross.

Our analysis of NNSA data shows that NNSA is focusing the majority of the program's resources on states with high curie amounts and large

²⁶NNSA defines material attractiveness levels for radiological material as the measure of risk based on the relative consequences if that material type and quantity were used in a dirty bomb. The goal of a risk-based approach is to ensure that the most attractive materials receive the most stringent protection.

numbers of hospitals and medical buildings with high-risk radiological sources. As of March 1, 2012, NNSA had spent \$53 million—or 51 percent of total expenditures for the Domestic Material Protection program—in Massachusetts, New York, Texas, Pennsylvania, and California. These five states contain 37 percent of all hospitals and medical facilities with high-risk radiological sources, and 39 percent of all curies in hospitals in the United States.

However, as table 2 shows, some states with large numbers of hospitals and medical facilities—Florida, Indiana, New Jersey, Ohio, and Tennessee—have not received as many upgrades from NNSA. These states received \$13 million, or 12 percent of all NNSA expenditures since the program began in 2008. Furthermore, other states with large numbers of medical facilities, such as Alabama, Michigan, and Wisconsin, have received no assessments or upgrades. In addition, some states with relatively few hospitals and medical facilities and a small amount of curies have each received more than \$1 million from NNSA to upgrade their facilities. These states were Hawaii and Rhode Island. In the case of Hawaii, NNSA officials told us that the state has over 50,000 curies of non-medical cesium-137, which made doing medical upgrades at the same time cost effective. In addition, NNSA said that Hawaii served as a model for how a network of facilities could be integrated into a centralized security network. As NNSA moves forward with the program, these officials said that they hope to replicate this model in some large cities and additional small states.

Table 2: NNSA Expenditures on Assessments and Upgrades by State, as of March 1, 2012

Dollars in thousands

State/U.S. territory	Number of medical facilities completed	Total cost of upgrades	Total number of medical facilities	Total number of curies	Percentage of total cost of upgrades
Massachusetts	25	\$11,366	72	138,809	11%
New York	41	11,358	110	251,210	11
Texas	45	11,338	121	10,257,731 ^a	11
Pennsylvania	36	10,691	95	185,368	10
California	26	8,267	162	328,339	8
Maryland	20	7,963	65	1,065,431 ^a	8
North Carolina	17	5,134	41	2,888,573 ^a	5
Florida	12	4,771	94	1,423,296 ^a	5
Washington	10	4,206	30	57,592	4
Illinois	15	3,872	48	127,625	4
Georgia	12	3,123	25	102,694	3
New Jersey	9	3,066	54	85,974	3
Tennessee	6	2,759	37	110,736	3

State/U.S. territory	Number of medical facilities completed	Total cost of upgrades	Total number of medical facilities	Total number of curies	Percentage of total cost of upgrades
Washington D.C.	5	2,068	9	27,637	2
Ohio	6	1,977	56	86,778	2
Colorado	7	1,820	24	60,372	2
Rhode Island	1	1,697	9	24,693	2
Missouri	3	1,492	24	45,633	1
Virginia	5	1,214	26	39,500	1
Connecticut	3	1,130	24	29,280	1
Hawaii	3	1,017	5	12,905	1
Montana	3	906	9	26,104	1
Arkansas	1	810	16	16,588	1
Oklahoma	3	703	12	28,964	1
Mississippi	2	691	13	14,837	1
Utah	4	657	16	26,278	1
Indiana	1	466	34	56,589	0
Alabama	0	0	26	16,249	0
Alaska	0	0	2	1,363	0
Arizona	0	0	5	26,070	0
Delaware	0	0	2	3,781	0
Idaho	0	0	3	3,282	0
Iowa	0	0	10	15,128	0
Kansas	0	0	9	21,748	0
Kentucky	0	0	9	21,471	0
Louisiana	0	0	13	28,449	0
Michigan	0	0	36	50,715	0
Minnesota	0	0	19	25,468	0
Nebraska	0	0	17	1,531,828 ^a	0
New Hampshire	0	0	4	12,220	0
New Mexico	0	0	17	6,768,686 ^a	0
Oregon	0	0	16	22,914	0
Puerto Rico	0	0	5	10,470	0
South Carolina	0	0	20	2,125,667 ^a	0
Vermont	0	0	3	1,917	0
West Virginia	0	0	9	7,265	0
Wisconsin	0	0	27	40,659	0
Maine	0	0	6	7,976	0
Nevada	0	0	5	3,346	0
North Dakota	0	0	5	5,787	0
South Dakota	0	0	2	16	0
Virgin Islands	0	0	1	10	0
Total	321	\$104,560	1,502	28,272,024	100

Sources: GAO analysis of NNSA and NRC data.

Note: The sum of the individual numbers may not equal the totals due to rounding.

^aThis state includes one or more panoramic irradiators with large curie activity sources.

NNSA officials told us that both the cost efficiencies and the voluntary nature of the Domestic Material Protection program require that they target sites based on their selection criteria and look for opportunities to provide upgrades when hospitals and medical facilities volunteer for assessments and upgrades. These officials stated that budgetary uncertainty makes it necessary to identify states where they can maximize their resources by upgrading a number of facilities in close proximity to each other. In addition, NNSA conducts outreach efforts in partnership with NRC and Agreement States to educate licensees about its program and find hospitals and medical facilities that want to participate. NNSA officials told us their outreach and promotional efforts are constrained because they do not want to enlist more facilities in the program than can be funded in a reasonable period of time. Additionally, NRC has supported NNSA's program by making licensees aware of the program in a January 2010 NRC Regulatory Issue Summary.²⁷ In the issue summary, NRC officials encouraged licensees to work cooperatively with manufacturers; regulators; and other federal, state, and local authorities to look for opportunities to further enhance the security of their sources and devices and incorporate best practices, where appropriate. The NRC officials also stated that NNSA staff and contractors have valuable perspectives and experience on best practices from visiting multiple licensees and operations. According to an NNSA official, increased collaboration with NRC and Agreement States to promote the program would be beneficial.

However, some Agreement States are more proactive than others in helping NNSA find such hospitals and medical facilities. For example, NNSA has not completed upgrades in some states with a large number of radiological sources, like Michigan and Wisconsin. The opposite is true in some states with fewer sources, such as Hawaii and Rhode Island, where NNSA found enough facilities to participate to make the upgrades cost effective.

²⁷NRC Regulatory Issue Summaries are used to (1) document NRC endorsement of resolution of issues addressed by industry-sponsored initiatives, (2) solicit voluntary licensee participation in staff-sponsored pilot programs, (3) inform licensee of opportunities for regulatory relief, (4) announce staff technical or policy positions not previously communicated to industry or not broadly understood, and (5) address matters previously reserved for administration letters.

Conclusions

A dirty bomb attack in the United States would have serious economic and psychological consequences. It is therefore in the interest of the federal government to ensure that all high-risk radiological materials in U.S. hospitals and medical facilities are secured as quickly as possible from potential theft or sabotage. However, NNSA does not expect to complete security upgrades at all hospitals and medical facilities in the United States until 2025; one-fifth of the upgrades are completed to date. In addition, the voluntary nature of NNSA's security upgrade program allows hospitals and medical facilities that contain high-risk radiological materials to refuse security upgrades, even though they are initially paid for by NNSA. As a result, 14 hospitals and medical facilities, with a combined 41,000 curies of high-risk radiological material, have declined to participate in the program, and several of these facilities are located in or in close proximity to populated urban areas. NNSA has taken steps to promote the program both by speaking at conferences and through other outreach efforts. In addition, NRC and Agreement States have provided support through promotion activities, such as NRC issuing a Regulatory Issue Summary in 2010 that described the NNSA program. These are positive steps, but there are still many hospitals that are not participating in this important program. While we understand that some hospitals and medical facilities may not participate in the program due to cost concerns, the longer the security upgrades remain unimplemented, the greater the risk that potentially dangerous radiological materials from these facilities could be used as a terrorist weapon.

NRC has taken a risk-based approach to improve the security of radiological sources at U.S. hospitals and medical facilities, but this approach is not based on facility specific security risks and results in a wide variety of security measures implemented by the medical facilities we visited. The risk-based requirements do not go far enough as several of the medical facilities we visited did not have adequate security measures in place. NRC's security controls are designed to improve security but do not prescribe the specific measures that licensees should take to secure their sources, such as specific direction on the use of cameras, alarms, and other physical security measures. As a result, these security controls, and the manner in which they are implemented, have left some hospitals and medical facilities we visited vulnerable to possible theft or sabotage of potentially dangerous radiological sources. Furthermore, NRC's pending regulations will require that licensees choose security measures to implement from a menu of options based on NRC's earlier implementation guidance. Similar to the current security requirements, the pending regulations do not specify which measures best address the risks posed by hospital radiological sources, allowing

medical facilities to potentially choose the least disruptive option for their operations or the most economical option regardless of the risk.

The limitations in NRC's security controls are exacerbated because NRC and Agreement State inspectors may not receive adequate training from the agency on the security of high-risk radiological material at hospitals and medical facilities. According to the views of several inspectors we interviewed—the 5 days of training provided by NRC is not sufficient for inspectors who typically have a health and safety background and limited security experience. According to NRC, the training is one component for qualification to perform independent security inspections. Other components include: 1) qualification as a NRC health and safety inspector, 2) observation of security inspections conducted by other experienced security inspectors, and 3) conducting an inspection under the direct oversight of a qualified security inspector. Nevertheless, the inspectors may not be in the best position to make the most informed decisions and judgments about the security of licensees' radiological materials. For example, we were told that an irradiator stored on a wheeled pallet located down the hall from a loading dock had not raised inspectors' concerns during the facility's most recent NRC security inspection. Moreover, some hospital officials, including RSOs, rely on inspectors for advice on how to implement NRC's security controls. However, these inspectors have minimal security training, and hospital officials receive limited security guidance from NRC in how to implement the security controls. Additional vulnerabilities are created because NRC security controls do not require that medical facility officials and RSOs have security experience. Without adequate security guidance, medical facility officials, including RSOs, who may be responsible for implementing NRC's security controls may not have adequate knowledge of securing equipment containing high-risk radiological sources. Finally, ensuring that hospitals only grant unescorted access to trustworthy individuals is critical to strengthening security, especially for securing against an insider threat. However, the current background examination process relies upon the judgment of hospital personnel, who may not have adequate experience to make that determination. For this reason, some hospital administrators told us that NRC should provide them with additional support for conducting background checks and making trustworthiness and reliability determinations as to which employees would have unescorted access to equipment containing high-risk radiological sources.

Recommendations for Executive Action

GAO is making four recommendations.

Because the security of radiological sources in hospitals and medical facilities has national security implications, and many potentially vulnerable medical facilities with high-risk sources have not received security upgrades, we recommend that the Administrator of NNSA, in consultation with the Chairman of NRC and Agreement State officials, take the following action:

- Increase outreach efforts to promote awareness of and participation in NNSA's security upgrade program. Special attention should be given to medical facilities in urban areas or in close proximity to urban areas that contain medical equipment with high-risk radiological sources.

In addition, to help address the security vulnerabilities at U.S. hospitals and medical facilities that contain high-risk radiological materials, we recommend that the Chairman of the Nuclear Regulatory Commission take the following three actions:

- Strengthen NRC security requirements by providing hospitals and medical facilities with specific measures they must take to develop and sustain a more effective security program, including specific direction on the use of cameras, alarms, and other relevant physical security measures.
- Ensure that NRC and Agreement State inspectors receive more comprehensive training to improve their security awareness and ability to conduct related security inspections.
- Supplement existing guidance for facility officials, including RSOs, who may be responsible for implementing NRC's security controls, in how to adequately secure equipment containing high-risk radiological sources and conduct trustworthiness and reliability determinations.

Agency Comments and Our Evaluation

We provided a draft of this report to the Chairman of NRC, the Administrator of NNSA, the Secretary of Defense, and the Secretary of Veterans Affairs. NRC provided written comments on the draft report, which are presented in appendix III. In addition, NRC provided technical comments, which we incorporated as appropriate. NNSA and VA did not provide written comments but provided technical comments which we incorporated as appropriate. DOD did not provide comments.

In its comments, NRC agreed with one of our four recommendations and neither agreed nor disagreed with the three other recommendations. Specifically, NRC agreed that the Administrator of NNSA, in consultation with NRC and Agreement state officials, increase outreach efforts to promote awareness of NNSA's security upgrade program, with special attention given to medical facilities in urban areas or in close proximity to urban areas that contain medical equipment with high-risk radiological sources.

NRC neither agreed nor disagreed with our other recommendations that it (1) strengthen its security requirements by providing hospital and medical facilities with specific measures they must take to develop and sustain a more effective security program; (2) ensure that NRC and Agreement State inspectors receive more comprehensive training to improve their security awareness and ability to conduct related security inspections; and (3) train facility officials who may be responsible for implementing NRC security controls in how to adequately secure equipment and conduct trustworthiness and reliability determinations. In its comments, NRC provided additional information regarding each of these three recommendations as follows:

Strengthening NRC security requirements. NRC stated that per its policy it uses a multilayered risk informed performance-based approach for the security of radioactive materials in the United States. It also stated in its comments that the requirements were developed in consultation with the Agreement States, in consideration of available intelligence reporting and security assessments performed by experts inside and outside the NRC, and are consistent with IAEA security guidelines and Executive Order 12866. We do not take issue with NRC's statement that its performance-based approach is consistent with IAEA security guidelines and Executive Order 12866. However, we note that a more prescriptive approach for the security of radioactive materials, such as that we are recommending, is also consistent with IAEA security guidelines. In fact, the guidelines point out that a performance-based approach functions most effectively where there are professional advisors with expertise to design and implement the necessary security measures, a situation we found not to exist in many of the medical facilities we visited. With respect to Executive Order 12866, we would also note that NRC states that the requirements of the order do not apply to it. However, even if the order did apply to NRC, the order itself provides only that "*to the extent feasible*" agencies should adopt a performance-based approach. The order further directs agencies to which the order applies to tailor their regulations to impose the least burden possible "*consistent with obtaining regulatory objectives.*" We found that NRC's current performance-based approach does not

consistently ensure that NRC is meeting its objective of securing high-risk radiological sources at the 26 selected hospitals and medical facilities we visited.

NRC also stated that in its view, our recommendation is based on four security issues identified in the report, two of which they identified as violations of the existing requirements. NRC states that the failure of a licensee to properly implement security controls established under a performance based regulatory requirement is a compliance issue, and does not mean that the intended control itself is inadequate. We recognize in our draft report that NRC has adopted a risk-based approach to radiological security and state that NRC's security requirements are non-prescriptive, which allows licensees to develop security programs specifically tailored to their facilities. However, as we also noted in our draft report, this risk-based approach is not based on security risks specific to hospitals and medical facilities and results in a wide variety of security measures implemented by the medical facilities we visited during the course of our audit work. Consequently, we found that some of the medical equipment in the facilities we visited was more vulnerable to potential tampering or theft than that of other facilities, even though all the facilities we visited had implemented NRC's security controls and undergone inspections by either NRC or Agreement State inspectors. Furthermore, we are not basing our recommendation, as NRC states, solely on our observations at 26 medical facilities. Rather, we are also relying on the views of law enforcement personnel from states with significant amounts of high-risk radiological material, who told us that NRC's security controls have an inherent weakness: the security controls do not specify what the facility is protecting against and are not linked to a design basis threat. In addition, NNSA has developed a specific program to upgrade the physical security at hospitals and medical facilities in the United States, which already meet NRC's security controls. In our view, it stands to reason that if NNSA has identified security vulnerabilities at 321 hospitals and medical facilities in the United States, and taken actions to address them, then NRC's existing security controls need to be strengthened. This is not merely an issue of how licensees comply with existing security regulations but involves both the security requirements and their implementation. For these reasons, we continue to believe our recommendation that NRC strengthen its security requirements is appropriate.

Additional training for inspectors. NRC stated that its training course provides instruction on a performance based methodology to evaluate and assess the adequacy of a physical protection system to protect against theft or sabotage of materials identified in NRC's security

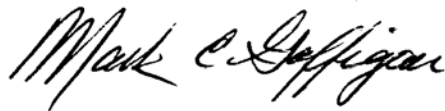
controls. NRC also stated that its one 5-day training course, in combination with on the job training and other requirements, prepares NRC and Agreement State inspectors to complete their required duties. NRC stated that it will evaluate whether any additional training enhancements are needed to its inspector qualification program based on our recommendation, and it plans to review and revise the training associated with the inspector qualification program in conjunction with pending security regulation. We are encouraged that NRC will evaluate whether any additional enhancements are needed to its inspector qualification program in response to our recommendation. We believe that NRC's review of its training is necessary and should be completed as quickly as possible, with an eye toward adopting a more comprehensive inspector training program, as envisioned in our recommendation.

Training for hospital personnel. NRC recognizes our concern that there is a need to improve the licensee's knowledge of acceptable security practices. According to NRC, as a regulator, it must maintain independent, objective oversight of licensees and may not operate in a consultative role. Therefore, NRC stated that it does not provide training to licensees but provides regulatory guidance documents to aid facility officials as they establish programs and specific controls to meet security requirements, including implementing guidance and over 200 questions and answers for the existing security requirements on its public website. However, as we stated in the draft report, even with this guidance, facility officials at 15 of the 26 hospitals and medical facilities we visited told us that they have limited security experience and no training from NRC on how to implement the security controls. In addition, the current background examination process (trustworthiness and reliability) relies on the judgment of hospital personnel, who may not have adequate experience to make that determination. Therefore, we continue to believe that medical facility officials would benefit from additional support from NRC when implementing the security controls at their facilities. Because NRC believes it cannot provide training to its licensees given its independent role as a regulator, we are modifying the recommendation to encourage NRC to supplement existing guidance and ensure that it is widely disseminated, rather than provide specific training to facility officials.

We are sending copies of this report to the Secretaries of the Departments of Defense, Energy, and Veterans Affairs; as well as the Administrator of the National Nuclear Security Administration; the Chairman of the Nuclear Regulatory Commission; the appropriate congressional committees; and other interested parties. In addition, the report is available at no charge on the GAO website at <http://gao.gov>.

If you or your staff members have any questions about this report, please contact me at (202) 512-3841 or gaffiganm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Sincerely yours,

A handwritten signature in black ink that reads "Mark E. Gaffigan". The signature is written in a cursive style with a large, stylized initial "M".

Mark Gaffigan
Managing Director
Natural Resources and Environment

Appendix I: Scope and Methodology

We focused our review primarily on the Nuclear Regulatory Commission (NRC) and the Department of Energy's National Nuclear Security Administration (NNSA) because they are the principal federal agencies with responsibility for securing radiological material at hospitals and medical facilities in the United States. We also performed work at the Departments of Defense (DOD), Homeland Security (DHS), Justice (DOJ), and Veterans Affairs (VA) because they are also involved in securing radiological material. In addition, we interviewed experts in the field of nuclear security, representatives from state government, and safety and security personnel at hospitals and medical facilities to discuss their views on how radiological material is secured at U.S. hospitals and medical facilities. In August 2011, we attended the Organization of Agreement States (OAS) annual meeting in Richmond, Virginia, where we spoke to Agreement State representatives and attended sessions on how states oversee the security of radiological material.

We visited hospitals and medical facilities in California, Maryland, New York, Pennsylvania, Tennessee, Texas, Virginia, and Washington, D.C. We selected these states and Washington D.C., on the basis of geographic dispersion, curies of radiological sources, number of buildings with high-risk radiological sources in the state, and number of sites with NNSA security upgrades completed or in progress. Overall, these seven states and Washington, D.C., contain over 12 million curies, or 43 percent of all curies in U.S. hospitals and medical facilities. In addition, the seven states and Washington, D.C., have 625 hospitals and medical buildings with high-risk radiological sources, or 42 percent of all medical sites with high-risk radiological material in the United States. As of March 1, 2012, NNSA spent almost \$56 million in the seven states and Washington, D.C., on assessing sites and completing upgrades, or 53 percent of the program's total expenditure. During our review, we observed physical security upgrades at 26 hospitals and medical facilities. These sites included university and private hospitals, medical research facilities, blood banks, and cancer treatment facilities. The 26 sites we visited are a non generalizable sample, selected on the basis of the number of radiological devices in the state and the total number of cumulative curies contained in these devices in each state. In addition, we considered if the site had undergone security upgrades funded by NNSA, and whether the site is located in a large urban area. At each location, we interviewed facility staff responsible for implementing procedures to secure radiological sources. We also met with security personnel at each site, when available, and spoke to officials with local law enforcement agencies responsible for responding to security breaches. We also met with local law enforcement personnel in Los Angeles County, New York City, and

Washington, D.C., to discuss coordination of security across large urban areas.

We received electronic data from NNSA's G-2 database, which aggregates data from NRC's National Source Tracking System (NSTS). To determine the reliability of these data, we conducted electronic testing and interviewed staff at NNSA and NRC about the reliability of these data. We tested these data to ensure both their completeness and accuracy, and determined that these data were sufficiently reliable to use in selecting locations to visit and summarizing by state the total number of buildings, number of buildings with completed security upgrades, and total number of curies.

To examine how NRC's regulations direct the security of high-risk radiological material at U.S. hospitals and medical facilities, we reviewed information and interviewed officials responsible for overseeing and securing sources at NRC, NNSA, VA, DOD, DHS, and DOJ. We also reviewed information from Agreement States and NRC regions and interviewed officials at 20 of the 37 Agreement States and the three NRC regional offices with responsibility for overseeing high-risk radiological material. We spoke with officials about how Agreement States implement the NRC security controls from the following 20 of the 37 Agreement States: Alabama, Arizona, Arkansas, California, Colorado, Florida, Kentucky, Maryland, Massachusetts, Mississippi, New Mexico, New York, North Carolina, Pennsylvania, Rhode Island, Tennessee, Texas, Virginia, Washington, and Wisconsin. We also spoke with officials in NRC Regions I, III, and IV. We selected the Agreement State and NRC Regional Office officials based on their experience with inspecting for the security of high-risk radiological sources across the United States.

To learn how NRC security requirements are implemented at the facilities, we visited hospitals, medical facilities, and local law enforcement agencies in the seven states and Washington, D.C., and interviewed officials about NRC's security requirements. To assess NRC's new rule, approved by the NRC on March 16, 2012, we reviewed the proposed regulation and spoke with NRC officials about its implementation. To determine the extent to which NRC and Agreement State inspectors receive security training, we discussed training procedures with NRC headquarters staff, reviewed training materials, and interviewed inspectors in NRC regional offices and Agreement States about the effectiveness of the training. To determine the sufficiency of staffing and resources in the 37 Agreement States, we reviewed 40 Integrated Materials Performance Evaluation Program (IMPEP) reports conducted

by NRC in 40 state programs or NRC regions from 2006 to 2011. We analyzed the IMPEP reports to assess how Agreement States are implementing NRC's security controls.

To evaluate the extent to which NNSA has enhanced the security of high-risk radiological sources at U.S. hospitals and medical facilities and the challenges they face, we analyzed information and interviewed NNSA officials about the Domestic Material Protection program, which provides voluntary upgrades to facilities with high-risk radiological material. We analyzed NNSA data outlining the number of facilities that have received upgrades or are in the process of receiving upgrades and visited facilities that have received NNSA upgrades and security assessments in California, New York, Pennsylvania, Tennessee, Texas, Virginia, and Washington, D.C. To assess the voluntary nature of the program and sustainability of the upgrades, we spoke with hospital and medical facility officials about the program. To assess NNSA's prioritization criteria and determine how much money the agency has spent on security enhancements, we gathered cost data from NNSA and contacted the agency officials who oversee the program. We also analyzed NNSA expenditure data to determine in which states NNSA has spent money on upgrades and assessments since the program began. We conducted electronic testing and discussed the reliability of these data with NNSA officials, and we determined that they were sufficiently reliable to summarize the total cost of the upgrades by state.

We conducted this performance audit from April 2011 to September 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: NRC Security Controls and Selected Pending Part 37 Regulations Changes (10 C.F.R. Part 37)

Relevant Increased Controls and Fingerprint Order	Selected Part 37 Changes
<p>Access controls (IC 1)</p> <p>Licenseses shall control access to radioactive material at all times and limit access only to trustworthy and reliable individuals, approved by the licensee, who require access to perform their duties.</p> <ul style="list-style-type: none"> The licensee shall allow only trustworthy and reliable individuals, approved in writing by the licensee, to have unescorted access to radioactive material quantities of concern and devices. The licensee shall approve for unescorted access only those individuals with job duties that require access to such radioactive material and devices. For individuals employed by the licensee for 3 years or less, trustworthiness and reliability shall be determined, at a minimum, by verifying employment history, education, and personal references. The licensee shall also, to the extent possible, obtain independent information to corroborate that provided by the employee (i.e., seeking references not supplied by the individual). For individuals employed by the licensee for longer than 3 years, trustworthiness and reliability shall be determined, at a minimum, by a review of the employees' employment history with the licensee. In the case of a service provider's employee, the licensee shall obtain from the service provider written verification attesting to or certifying the employee's trustworthiness and reliability from an NRC-required background check before granting unescorted access. 	<ul style="list-style-type: none"> Generally, the reviewing official must also be fingerprinted and undergo or have undergone an FBI criminal history check. Individuals who have been determined to be trustworthy and reliable must undergo training in the licensee's security program and procedures. The background check must cover the past 7 years (or since 18th birthday if shorter) for all employees, whether the individual is a long-time employee or a new hire. Individuals must be reinvestigated every 10 years. Part 37 provides relief from record checks and background investigations for certain categories of service provider employees (emergency response personnel, commercial vehicle drivers, and package handlers at transportation facilities).
<p>Monitor and Response (IC 2)</p> <p>Licenseses shall have a documented program to monitor and immediately detect, assess, and respond to unauthorized access to radiological sources.</p> <ul style="list-style-type: none"> The licensee shall respond immediately to any actual or attempted theft, sabotage, or diversion of such radioactive material or of the devices, including requesting assistance from local law enforcement. The licensee shall have a prearranged plan with their Local Law Enforcement Agency for assistance in response to an actual or attempted theft, sabotage, or diversion of such radioactive material or of the devices consistent with scope and timing with a potential vulnerability. The licensee shall have a dependable means to transmit information between, and among, the various components used to detect and identify an unauthorized intrusion, to inform the assessor, and to summon the appropriate responder. After initiating appropriate response to any actual or attempted theft, sabotage, or diversion of radioactive material or of the devices, the licensee shall, as promptly as possible, notify NRC Operations Center. 	<p>A written security plan, rather than a documented program is required.</p> <ul style="list-style-type: none"> Licenseses must conduct training on their security procedures. Monitoring and detection must be performed by: <ul style="list-style-type: none"> (i) A monitored intrusion detection system that is linked to an on-site or off-site central monitoring facility; or (ii) Electronic devices for intrusion detection alarms that will alert nearby facility personnel; or (iii) A monitored video surveillance system; or (iv) Direct visual surveillance by approved individuals located within the security zone; or (v) Direct visual surveillance by a licensee designated individual located outside the security zone. Licenseses must assess any suspicious activity related to possible theft, sabotage, or diversion of radioactive material and notify NRC and local law enforcement as appropriate. Licenseses must implement a maintenance and testing program to ensure that monitoring and detection equipment is functioning properly. Licenseses are required to periodically (at least annually) review the security program to ensure its continuing effectiveness. Licenseses must have a means to detect unauthorized removal of the radioactive material from the security zone.

**Appendix II: NRC Security Controls and
Selected Pending Part 37 Regulations Changes
(10 C.F.R. Part 37)**

Relevant Increased Controls and Fingerprint Order	Selected Part 37 Changes
<p>Documentation (IC 5) Licensees shall retain documentation required by the Increased Controls for 3 years after they are no longer effective.</p>	No substantive changes.
<p>Protection of Sensitive Information (IC 6) Detailed information generated by licensees that describes the physical protection of radioactive material quantities of concern is sensitive information and shall be protected from unauthorized disclosure.</p>	<ul style="list-style-type: none"> When not in use, the licensee shall store its security plan and implementing procedures in a manner to prevent unauthorized access. Information stored in nonremovable electronic form must be password protected
<p>Fingerprint Order</p> <ul style="list-style-type: none"> Individuals with unescorted access must be fingerprinted and undergo a Federal Bureau of Investigations (FBI) criminal history check. The official responsible for determining whether individuals are trustworthy and reliable must also undergo a trustworthiness and reliability determination. 	<ul style="list-style-type: none"> The reviewing official must also be fingerprinted and undergo an FBI criminal history check

Sources: GAO analysis of Order Imposing Increased Controls (NRC Order EA-05-090), Order Imposing Fingerprinting (NRC Order EA-07-305), and 10 C.F.R. Part 37 Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material.

Note: In 2005, NRC issued two security orders containing additional requirements for securing radioactive materials during transport. Changes to these orders in Part 37 are not included in this table.

Appendix III: Comments from the Nuclear Regulatory Commission



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

August 28, 2012

Mr. Glen Levis, Assistant Director
U.S. Government Accountability Office
Natural Resources and Environment
Room 2T23
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Levis:

Thank you for the opportunity to review and comment on the draft of your report GAO-12-925, "Nuclear Nonproliferation: Additional Actions Needed to Improve Security of Radiological Sources at U.S. Medical Facilities," which the U. S. Nuclear Regulatory Commission (NRC) received on August 9, 2012. The NRC staff has compiled specific technical comments on the report which are provided in the enclosure.

The U.S. Government Accountability Office (GAO) report concludes that the NRC's security controls need to be strengthened because they do not prescribe specific security measures that the licensees should take to secure their radiation sources, such as specific direction on the use of cameras, alarms, and other physical security measures. The GAO further concludes that NRC and Agreement State inspectors may not receive adequate training from the agency on the security requirements for risk-significant radiological material at hospitals and medical facilities. In addition, the GAO provides four recommendations, one primarily directed to the Administrator of the National Nuclear Security Administration (NNSA) and three which recommend specific action by the NRC. The NRC comments on the recommendations are listed below.

- GAO Recommendation: The Administrator of NNSA, in consultation with the Chairman of the NRC and Agreement State officials, increase outreach efforts to promote awareness of and participation in NNSA's security upgrade program. Special attention should be given to medical facilities in urban areas or in close proximity to urban areas that contain medical equipment with high-risk radiological sources.

NRC Response: The NRC agrees with this recommendation and will continue to support the NNSA's outreach activities to promote licensee awareness of and participation in the security upgrade program within the limits of our authorities and available resources.

- GAO Recommendation: Strengthen NRC security requirements by providing hospitals and medical facilities with specific measures they must take to develop and sustain a more effective security program, including specific direction on the use of cameras, alarms, and other relevant physical security measures.

NRC Response: NRC acknowledges GAO's recommendation favoring a more prescriptive set of security measures. However, consistent with long established Commission policy and practice and Executive Order 12866 of September 30, 1993, "Regulatory Planning and Review," the NRC and the Agreement States use a multilayered risk informed performance-band approach for the security of radioactive materials in the United States. The requirements were developed in consultation with the Agreement States, in consideration of

G. Levis

- 2 -

available intelligence reporting and security assessments performed by experts inside and outside the NRC, and are consistent with the International Atomic Energy Agency (IAEA) "Code of Conduct on the Safety and Security of Radioactive Sources," and IAEA Nuclear Security Series No. 11, "Security of Radioactive Sources Implementing Guide." The requirements provide a framework that requires licensees to develop a security program with measures that provide adequate security, and are specifically tailored to each facility. Key requirements of the program include:

- Background checks, including fingerprinting to help ensure that individuals with unescorted access to radioactive materials are trustworthy and reliable.
- Controlling personnel access to areas where radioactive materials in quantities of concern are stored and used. Access must be limited to individuals that require access to the area and are deemed trustworthy and reliable, based on a background and criminal history check.
- Documented security programs that are designed with defense in depth to detect, assess and respond to actual or attempted unauthorized access events.
- Coordination and response planning between the licensee and local law enforcement agencies for their jurisdiction.
- Coordination and tracking of radioactive materials shipments.
- Security barriers to discourage theft of portable devices that contain radioactive materials in quantities of concern.

Compliance with security requirements is verified during regular inspections conducted by trained NRC and Agreement State inspectors. The licensees are required to implement corrective actions when violations are identified, and these corrective actions are then verified and evaluated during subsequent inspections.

The report identifies four security issues as a basis for recommending NRC use more prescriptive security requirements rather than the current performance based requirements. Two of these issues are clear violations of existing security requirements for access control (a lock combination on the door frame) and access authorization (failing to know and to limit who is authorized for access to a controlled room). The failure of a licensee to properly implement security controls established under a performance based regulatory requirement is a compliance issue, and does not mean that the intended control itself is inadequate. Insufficient information has been provided to NRC regarding the other two examples to determine whether there are violations of security requirements. For example, the irradiator device mounted on wheels was not necessarily vulnerable if it was locked inside a secure room with appropriate access control and other security measures. Also of note, the new 10 CFR Part 37 rule, when implemented, will require two independent physical controls that form tangible barriers to secure the material from unauthorized removal when the device is not under direct control and constant surveillance by the licensee in order to delay removal of mobile devices. The NRC and the Organization of Agreement States (OAS) have a shared concern over these issues, and have requested additional information concerning the security issues identified in the report, to permit follow-up and appropriate action.

Security and control of radioactive materials is a top priority for the NRC. The NRC, in coordination with Agreement State regulators, has developed a robust program of security measures for radioactive materials that is focused on providing protection commensurate

G. Levis

- 3 -

with the threat and risk associated with the material. The United States is the first country in the world to require such enhanced security requirements for radioactive materials, and both Federal and State regulators ensure that such materials remain secure. While no security program provides absolute security, the security of risk-significant radioactive materials at medical facilities in the United States has greatly improved since the terrorist attacks of September 11, 2001.

- GAO Recommendation: Ensure that the NRC and Agreement State inspectors receive more comprehensive training to improve their security awareness and ability to conduct related security inspections.

NRC Response: The "NRC Materials Control, Security Systems and Principles (Increased Controls)" course provides instruction on a performance based methodology to evaluate and assess the adequacy of a physical protection system to protect against theft or sabotage of materials identified in the Increased Controls. This, combined with on the job training and other requirements, prepares NRC and Agreement State inspectors to complete their required duties.

The NRC will evaluate whether any additional enhancements are needed to our inspector qualification program based on GAO's recommendation. Currently, the NRC plans to review and revise the inspector qualification program for radioactive materials security inspections, to include the associated training, to support the implementation of the 10 CFR Part 37 rule. The Commission approved the final rule in March 2012. The rule package, including draft guidance, is with the Office of Management and Budget for review. The rule is expected to be published in the *Federal Register* by the end of calendar year 2012. NRC licensees have up to 1 year from the date of publication to be in compliance with Part 37 requirements. The Agreement States have up to 3 years from publication to adopt compatible legally binding requirements.

- GAO Recommendation: Train facility officials, including RSOs, who may be responsible for implementing NRC's security controls, in how to adequately secure equipment containing high-risk radiological sources and conduct trustworthiness and reliability determinations.

NRC Response: The NRC understands the GAO's concern that there is a need to improve the licensee's knowledge of acceptable security practices. However, as a regulator, the NRC must maintain independent, objective oversight of licensees and may not operate in a consultative role with the licensees. Accordingly, we do not provide training to licensees. We do provide regulatory guidance documents that aid licensees as they establish programs and specific controls to meet requirements. To that end, the NRC has provided a great deal of security guidance to licensees. The NRC public website contains implementing guidance and over 200 questions and answers for the existing security requirements. The guidance document that will accompany the new 10 CFR Part 37 rule addresses each section of the rule.

As a world leader in the regulation of nuclear and radioactive materials, the NRC will continue its efforts to improve the security of radioactive sources, in coordination with Federal, State and International partners. We will continue to evaluate the current threat environment to ensure that security rules and regulations are risk-informed, appropriate and effective. The enclosed

**Appendix III: Comments from the Nuclear
Regulatory Commission**

G. Levis

- 4 -

comments from the NRC and the OAS are intended to provide a more comprehensive perspective related to the conclusions and recommendations contained in the draft report. Should you have any questions concerning these comments, please contact Jesse Arildsen at 301-415-1785.

Sincerely,



R. W. Borchardt
Executive Director
for Operations

Enclosure:
NRC Comments on the Draft
Government Accountability Office
Report (GAO-12-925)

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Mark Gaffigan (202) 512-3841 or gaffiganm@gao.gov

Acknowledgments

In addition to the contact name above, Gene Aloise (Director); Glen Levis (Assistant Director); Jeffrey Barron; Alysia Davis; Will Horton; Karen Keegan; Cheryl Peterson; Rebecca Shea; and Carol Hernstadt Shulman made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

