6/29/2010
75FR37483 (4)

PUBLIC SUBMISSION

As of: December 08, 2010
Received: December 08, 2010
Status: Pending_Post
Tracking No. 80bb1839
Comments Due: December 17, 2010
Submission Type: Web

Docket: NRC-2010-0209
Request for Comment on the Draft Policy Statement on the Protection of Cesium-137 Chloride Sources and Notice of Public Meeting

Comment On: NRC-2010-0209-0001
Request for Comments on Draft Policy Statement on the Protection of Cesium-137 Chloride Sources and Notice of Public Meeting

Document: NRC-2010-0209-DRAFT-0003
Comment on FR Doc # 2010-15734

Submitter Information

Name: Stephen Musolino
Address:
5 Smythe Court
Bellport, NY, 11713

General Comment

Subject: Docket ID NRC-2010-0209

In addition to the slides from my oral presentation at the workshop, two additional documents are attached:

1. Best Practices for Securing Radioactive Materials, BNL-90329-2009
2. Editorial on cesium chloride that was submitted for publication in the Health Physics Journal on November 29, 2010.

Attachments

NRC-2010-0209-DRAFT-0003.1: Comment on FR Doc # 2010-15734
NRC-2010-0209-DRAFT-0003.2: Comment on FR Doc # 2010-15734

SUNSI Review Complete
Template = ADM-013

E-RIDS = ADM-03
Add = J. Jankovich (JPJ2)
S. Hawkins (Sch2)

BROOKHAVEN
NATIONAL LABORATORY

BNL-90329-2009

Best Practices for Securing Radioactive Materials

Stephen V. Musolino and Daly T. Coulter[†]

May 15, 2009

Nonproliferation and National Security Department
Nonproliferation and Safeguards Division/Office 197C

† PHROUBUS, Inc.
2428 Sterling Point Drive
Portsmouth, VA 23703

Brookhaven National Laboratory
P.O. Box 5000
Upton, NY 11973-5000
www.bnl.gov

ACKNOWLEDGEMENT AND DISCLAIMER

This report is original material from collaboration between the Brookhaven National Laboratory and PHROBUS, Inc., which was partially funded by the New York City Department of Health and Mental Hygiene and the U.S. Department of Homeland Security. It incorporates experience by the authors in programs by the Department of Energy Global Threat Reduction Initiative and the U.S. Department of Homeland Security. The contents of this publication are solely the responsibility of the authors and do not necessarily represent the official vies of the New York City Department of Health and Mental Hygiene.

PURPOSE

The purpose of this document is to describe best practices available to manage the security of radioactive materials (RAM) in medical centers, hospitals, and research facilities. There are thousands of such facilities in the United States, and recent studies suggest that these materials may be vulnerable to theft or sabotage. Their malevolent use in a radiological-dispersion device (RDD), viz., a dirty bomb, can have severe environmental- and economic- impacts, the associated area denial, and potentially large cleanup costs, as well as other effects on the licensees and the public. These issues are important to all Nuclear Regulatory Commission and Agreement State licensees, and to the general public. This document outlines approaches for the licensees possessing these materials to undertake security audits to identify vulnerabilities in how these materials are stored or used, and to describe best practices to upgrade or enhance their security.

Best practices can be described as the most efficient (least amount of effort/cost) and effective (best results) way of accomplishing a task and meeting an objective, based on repeatable procedures that have proven themselves over time for many people and circumstances. Best practices within the security industry include information security, personnel security, administrative security, and physical security. Each discipline within the security industry has its own "best practices" that have evolved over time into common ones. With respect to radiological devices and radioactive-materials security, industry best practices encompass both physical security (hardware and engineering) and administrative procedures. Security regimes for these devices and materials typically use a defense-in-depth- or layered-security approach to eliminate single points of failure. The Department of Energy, the Department of Homeland Security, the Department of Defense, the American Society of Industrial Security (ASIS), the Security Industry Association (SIA) and Underwriters Laboratory (UL) all provide design guidance and hardware specifications. With a graded approach, a physical-security specialist can tailor an integrated security-management system in the most appropriate cost-effective manner to meet the regulatory and non-regulatory requirements of the licensee or client.

BACKGROUND

Although licensees in throughout the United States use both low-activity and high-activity RAM, the latter RAM poses the greatest public-health risk, both in its dispersed and solid form. High-activity radiation sources are used widely in a range of applications, such as scientific- and medical-research, nuclear medicine, and treating cancer.

Table 1 gives examples of devices of regulatory- and security- concern because of the quantity of radioactive material that each contains.

Table 1: Common High-activity Radiological Devices

Device	Radioisotope	Activity Range (Ci)**
Teletherapy	Cobalt 60 Cesium 137*	1000 – 15000
Irradiators	Cesium 137 Cobalt 60	1000 – 12000 1500 – 3000
Gamma Knife	Cobalt 60	1500 – 3000
High-dose-rate Brachytherapy	Iridium 192 Cesium 137* Cobalt 60	5 – 12 3 – 8 5 – 20

* No longer commercially available in the United States
**Activity range taken from IAEA TECHDOC 1344, Appendix II

Historically, the regulations only addressed hazards to health and safety from radiation sources to the control of routine- and accidental-exposure of personnel. A facility's Radiation Safety Officer (RSO) or his/her equivalent was responsible for managing this risk. Today, with the constant threat of terrorism, the RSO is now also responsible for the security RAM. Although RSOs may have extensive experience in health physics and industrial safety, experience showed that often their knowledge of security practices and technology is limited. The RSO must rely on support from within the facility, normally the security manager and their response force; outside the facility, the regulatory and licensing organization generally oversees the safety and security of the devices. Planning for the security of RAM also requires coordination with local law-enforcement agencies. This document provides information to help the responsible facility staff to

- Better assess and understand the vulnerabilities of the facilities where these materials are used;
- Outline the process for identifying these vulnerabilities;
- Identify options for enhancing the security of sources by applying administrative- and engineering-controls.

US Nuclear Regulatory Commission's Increased Controls

In response to the September 11, 2001 attack, and recognizing that high-activity radiation sources could be used malevolently, the NRC developed requirements for Increased Controls (IC) over radioactive sources that exceed the Quantities of Concern listed in Table 2. The IC are intended to reduce the risk of theft or unauthorized use, and to mitigate the potentially high and detrimental consequences to public health and safety. The IC, established in January 2006 and effective May 2006, were established to delineate licensees' responsibility to maintain control of licensed material and secure it from unauthorized removal or access. Details on these ICs are presented in NRC EA-05-090, SUBJECT: ISSUANCE OF ORDER FOR INCREASED CONTROLS FOR

CERTAIN RADIOACTIVE MATERIALS LICENSEES dated November 14, 2005. In summary, the ICs include descriptive requirements and suggestions for the following:

- Controlling Access; including trustworthiness and reliability of personnel
- Monitoring, Detecting, Assessing, and Responding;
- Transportation Requirements;
- Physical Barriers for Portable- and Mobile-Devices;
- Documentation, and Document Retention; and,
- Information Protection

Table 2: Radionuclides of Concern

Radionuclide	Quantity of Concern (TBq)[1]	Quantity of Concern (Ci)[2]
Am-241	0.6	16
Am-241/Be	0.6	16
Cf-252	0.2	5.4
Cm-244	0.5	14
Co-60	0.3	8.1
Cs-137	1	27
Gd-153	10	270
Ir-192	0.8	22
Pm-147	400	11,000
Pu-238	0.6	16
Pu-239/Be	0.6	16
Ra-226[5]	0.4	11
Se-75	2	54
Sr-90 (Y-90)	10	270
Tm-170	200	5,400
Yb-169	3	81
Combination of radioactive materials listed above[3]	See Footnote Below[4]	

1 The aggregate activity of multiple, collocated sources of the same radionuclide should be included when the total activity equals or exceeds the quantity of concern. See footnote 4 for the method of evaluation.

2 The primary values used for compliance with this Order are TBq. The curie (Ci) values are rounded to two significant figures for informational purposes only.

3 Radioactive materials are to be considered aggregated or collocated if breaching a common physical-security barrier (e.g., a locked door at the entrance to a storage room) would allow access to the radioactive material or devices containing the radioactive material.

4 If several radionuclide are aggregated, the sum of the ratios of the activity of each source, of radionuclide, *n*, A (*i,n*), to the quantity of concern for radionuclide *n*, Q(*n*), listed for that radionuclide equals or exceeds one. [(Aggregated source activity for radionuclide A) ÷ (quantity of concern for radionuclide A)] + [(aggregated source activity for radionuclide B) ÷ (quantity of concern for radionuclide B)] + etc........ >1. For example, if a licensee possessed two sealed sources , 10 Ci of ^{241}Am and 11 Ci of ^{192}Ir, the aggregate (sum of the fractions) would be 10/16 + 11/22 = 1.13. Therefore, while each sealed source is less than the Quantity of Concern, the sum of the fractions exceeds one equivalent Quantity of Concern, and the licensee is required to comply with the Increased Controls.

5 On August 31, 2005, the NRC issued a waiver, in accordance to Section 651(e) of the Energy Policy Act of 2005, for the continued use and/or regulatory authority of Naturally Occurring and Accelerator-Produced Material (NARM), which includes Ra-226. The NRC plans to terminate the waiver in phases, beginning November 30, 2007, and ending on August 7, 2009. The NRC has authority to regulate discrete sources of Ra-226, but has refrained from exercising that authority until the date of an entity's waiver termination. For entities that possess Ra-226 in quantities of concern, this Order becomes effective upon waiver termination. For information on the schedule for an entity's waiver termination, please refer to the NARM Toolbox website at http://nrcstp.ornl.gov/narmtoolbox.html.

The original IC Order required licensees to determine whether each person who requires unescorted access to radioactive material in quantities of concern to perform their job is trustworthy and reliable. The IC Order stated that this assessment must be based on work history, education, and personal references. Since conducting the initial IC compliance inspections, the NRC issued an additional order imposing requirements for fingerprinting and background checks for criminal history. This constitutes another factor, which licensees must consider in evaluating trustworthiness and reliability before determining whether an individual may be allowed unescorted access to radioactive material in quantities of concern. Fingerprints must be taken by local law-enforcement or an authorized agent, while the Federal Bureau of Investigation undertakes the background checks.

MANAGING THE SECURITY OF RADIOACTIVE MATERIAL

Terms must be defined to establish common ground among security specialists conducting the assessment. **Threat** is an **identifiable** and **credible** source of danger or loss, such as any opposing force, condition, source, or circumstance that potentially may negatively impact or degrade the accomplishment of business or mission. **Vulnerability is** exposure to an attack, a gap in security, oversights or omissions in device protection; considering the level of exposure to a threat identifies it, and the level of protection associated with that device. **Consequences** are the environmental-, health-, and economic-impacts of a RDD constructed with a given radioactive source.

Managing the security of radioactive sources begins with a full understanding of what the process involves. The approach to, and foundation of a good management plan is to conduct a security assessment of the entire facility, and not just the device, and storage facility, focusing primarily on the high-activity devices, and other radiological sources used in operations. Importantly, the Director of Security and the RSO should undertake this assessment together. As well as evaluating the local environment where RAM is located, overall risk of the facility is assessed, wherein *risk* is a function of *threat, vulnerability,* and *consequences.* Therefore, the review process will cover the following:

- Survey all devices that meet the high-activity criteria for Increased Controls as stated by the NRC and the DOHMH;
- Inspect other uses of sealed- or dispersible-RAM in the entire facility;
- Identify, assess, and analyze the *threat;*
- Lacking any specific threat, use the default threat of one knowledgeable insider, and two armed outsiders.
- Assess the *consequences* of theft or sabotage of high- and low-activity sources. Even though they may not be catastrophic, l*ow-activity* sources still might disrupt the operational continuity of a facility;
- Determine and evaluate vulnerabilities;
  - Vulnerabilities can be assessed at the source/point of use, and the facility as a whole;
- Identify and determine the resulting *risk*;
- Recommend actions necessary to mitigate and lower the levels of risk, i.e., propose plans, policies, administrative procedures, and best practices to manage the *risk*;

Facility security-managers often are challenged in making a quantifiable argument to senior management for improving security. With no recent incidents in or around a facility, such as an increase in crime or vandalism, presenting a successful case to modify physical security and/or policy or procedures can be difficult because there may be no direct correlation to productivity, security, or safety. Regardless, the security manager and the support team must press their argument by continually assessing the security risks that face the site. Employing the best security-practices assures the maintenance of the highest state of security for the facility. The resulting defense-in-depth approach, utilizing layered security, offers the best opportunity for establishing an integrated security management system. The definition of risk is a function of *threat, vulnerability,* and *consequences*. With this concept of risk, potential scenarios can be semi-quantitatively or relatively ranked to judge where facility-specific investments in security upgrades may be beneficial.

DEFENSE-IN-DEPTH

Defense-in-depth is a layered security system incorporating trained security personnel, technology, and administrative procedures to ensure a complete, functional system. The following are the elements of this approach:

- Detect: Detect unauthorized access [intruder(s)] to the RAM;
- Delay: Delay the intruder(s) by keeping them away from the devices and the RAM;
- Respond: Respond to the intruder(s) using in-house assets, and the local law-enforcement agency to interdict the intruder(s) before they gain direct access to any RAM and depart from the facility.

Systematically, this means installing technical upgrades and integrating people, procedures, and equipment. Detailed descriptions of detect, delay, and respond are given below:

Detect

Detection of an attempted theft of a device or other radioactive sources should occur as early as possible. It will maximize the effectiveness of installed access-delay elements encountered by the adversary later in the sequence, and improve the response force's effectiveness. To increase the probability of detection, multiple, complementary layers of detection should be installed, each employing a different technology.

The simplest form of intrusion detection is from human observation. Properly trained security personnel and staff who are well aware of suspicious activities, and know what actions to take if they observe them constitute a simple, effective, and inexpensive detection upgrade. For a typical high-activity device, the first layer of detection should be a door position sensor, usually a Balanced Magnetic Switch (BMS), installed on the door leading into the room containing the device.

The second layer of detection should be a complementary volumetric sensor (motion detector) located in all access passageways or corridors leading to the device, e.g. the labyrinth into a teletherapy room.

A third layer of detection, a penetration sensor, should be installed directly on the device. This layer of detection is critical because in some cased like the conduct of patient care in medical facilities, this situation typically require disabling some technical means of detection during normal working hours. This type of sensor would not have to be disabled, and will remain in the secure mode to protect the device.

The final layer could be duress buttons sited at key locations inside and around the room containing the high activity device, allowing staff to immediately signal unusual activities to security personnel.

Intrusion detection is not complete without verification and assessment. The latter is essential for detection-system elements that are subject to (false) alarms generated innocently, such as at perimeter-intrusion detection systems. Therefore, there must be some means of verifying and assessing the alarms. Alarms can be displayed in several ways, such as strobe lights, sirens, light panels, or displays at central alarm stations. The most practical method of evaluating an alarm is by closed circuit television cameras (CCTV). (Supplemental lighting from a protected power- source may be an essential component of a CCTV system.) The capability for remote assessment allows the security force to verify the alarm immediately, and without unknowingly exposing itself to potential hostile action, Further, it provides forensic information should a retrospective investigation be needed.

Delay

After detecting an adversary, installed delay elements help to prevent the completion of the malevolent act, and provide time for response forces to arrive and interdict the intruder. During working hours, a hardened door with high-strength locks leading into the room containing the device may be required to delay access. However, these alone will not effectively delay intruders during non-working hours unless there are some means of detecting an adversary attempting to penetrate the door.
Many consider the device itself to be the best approach for delay. Detection methods may be bypassed by an insider-threat. This puts additional pressure on the security force. The device may weigh several thousand pounds, but still may be vulnerable to removal of the source. Therefore, some physical-delay mechanism may be called for to insure the security of the device and source.

Response

The security force and its ability to respond to an incident are the critical elements in any defense-in-depth system. Not all security forces are created, funded, or equipped equally. This inconsistency necessitates close analysis to overcome any shortfalls in training or equipment. Within the United States, individual states generally regulate armed security forces, but this may vary, and so cause confusion when an assessment team completes their observations. Regardless of whether a response force is armed or not, the local law-enforcement agency plays a key role in interdicting and arresting the intruder(s). Should the source be removed from the device and taken out of the facility, the problem is far greater than if the source is recovered at the facility.

The following are the key criteria for a good response force:

- Properly selecting personnel;
- Providing the best training available;
- Supplying proper equipment and supporting materials;
- Conducting operations from a hardened central-alarm station;
- Ensuring correct procedures and post orders;
- Holding appropriate response-drills and exercises;
- Establishing a strong working relationship with local law-enforcement agencies;
- Securing strong support from facility management;
- Setting up a close working relationship with the RSO.

These criteria, coupled with strong support from facility management, will result in a capable response force that can contain and interdict an adversary.

CONDUCTING THE SECURITY ASSIST VISIT

Conducting a security-assist visit can take several hours or several days, depending on the size of the facility and the depth of the survey. Before conducting the survey, the assist-visit team meets the facility's key personnel, as appropriate. They normally include, but are is not limited to

- Radiation Safety Officer
- Director of Security
- The facility's Administrator, or designated representative
- Director of Human Resources
- Director of Research
- Director of Nuclear Medicine/Radiation Oncology or designated representative
- Director of Emergency Management, or designated representative
- Director of Safety, or designated representative
- Representative from the local licensing or regulatory agency
- Representative from the local law-enforcement agency

The assist-visit team reviews the scope of the survey and answer questions about the presentation of the findings. The participants discuss and agree upon the basis of threats to the facility. For example, under certain conditions, any high-activity device could be used to make an RDD. The threat may vary at each facility, but, in general, all unsecured high-activity devices may be at risk of theft or sabotage. While fixed devices usually are considered secure because of their size and weight, recent studies revealed that high-activity radioactive sources can be removed from very large, heavily shielded devices much quicker than originally assumed. Therefore, specifying a threat scenario is very important to the conduct of the survey. Without such high-activity devices, the theft and/or dispersal of smaller amounts of RAM would bring unwanted media attention to the facility, as well as the possible temporary loss of continuity of operations.

The assist-visit team will rely on regulatory, licensing, and local law-enforcement sources for a threat brief. Lacking an identified threat, the assessment team will use a default threat of "Theft or Sabotage of Radiological Sources" wherein one "knowledgeable insider" and two "armed outsiders" pose the threat. To mitigate risk, the facility would use access-control measures to control and monitor access, with sensors to "detect" intruders (and assessment systems to confirm the alarm's validity). Physical-security measures would secure the perimeter surrounding the sources (hardened doors and locks) to "delay" the intruders long enough for the response force supported by local law-enforcement to interdict and apprehend the intruders before they remove the RAM. In this context, barriers or hardened systems provide meaningful delay only after the attack is detected and confirmed. Should an attack on a barrier be undetected or unrecognized, the barrier may provide no useful delay for summoning or mobilizing a response force to interdict the attackers. Note that the assumption of one insider and two outsiders is a "minimum threat" level. A larger intruder force would require other security measures to mitigate the risk. Once the threat is agreed upon, the assist-visit team will begin their survey.

The team will require the assistance and accompaniment of knowledgeable facility representatives. Normally, the facility security-manager and the RSO will tour the facility with them to answer questions on the security practices in use, and about specific high-activity devices and other RAM in use or storage.

The team will focus on reviewing existing physical-security measures and material-control procedures to determine if there are vulnerabilities and resulting risks to the source. They will make observations and recommendations on procedural- and hardware-improvements to mitigate any risks to the source(s). Their focus will be on

1. **Devices and sources at the facility**
   - The number and types of devices
   - The quantity and activity of radiological sources
   - The material form of the isotopes
   - Transportation protocols for shipping sources
   - Locations, buildings/rooms

2. **Current Site-level Security**
   - Physical-security measures
   - Access-control measures, including visitor access
   - Key and card control
   - Radiation-detection systems
   - CCTV and other surveillance- or alarm-assessment systems
   - Delay/barrier elements
   - Licensee's controlled area/security zone area
   - Coordination with local law-enforcement agencies

3. **Material Control and Accountability Measures**
   - Radioactive material monitoring
   - Inventory and waste management
   - Tamper-indicating devices
   - Inventory- record Systems
     Procedures for transferring internal and external radioactive materials

Upon completing their survey and gathering data, the team will brief appropriate facility personnel about regarding their findings, presenting them as observations and recommendations as proposed changes and upgrades for the facility administrator to consider. The recommendations may cover changes to policies and procedures as well as to hardware upgrades that will improve security. After finishing the security-assist visit, team members will be prepared to discuss measures for physical-security upgrades with vendors, describing the suitability of equipment and installation procedures at the facility, and evaluating the effectiveness of the upgrades after their installation.

Observations and Recommendations

While all facilities that have one or more high-activity devices and possibly a variety of lower activity RAM are unique, they have common, consistent similarities. The recommendations from the assessment team generally will fall into four categories:

1. Facility policy
2. Security procedures
3. Physical-security hardware upgrades
4. Employee training

The facility management may not implement all of the assist team's recommendations immediately, and may never establish some of them. The team's emphasis is not expenditure of resources, but rather, to improve security awareness and to identify physical-security upgrades that will insure a comprehensive integrated security package. The following common recommendations generally apply to most, if not all facilities that contain RAM:

Facility Policy

A close review and updating of facility policies is the most cost-effective security measure available. The policies most impacted are the following ones:

- Employee hiring policy, including background check and random drug-testing
- Access control policy, including authorized exclusion list for personnel access
- Incident reporting policy
- Security-force incident response policy
- Disaster recovery policies
- Memorandum of Agreement with local law-enforcement agencies
- Control of sensitive information, including institutional websites accessible by the public

Security Procedures

The following security procedures are critical to the actions taken to prevent an incident, as well as those taken to respond to it.

- Response force's security post orders and procedures
- Security training procedures
- Alarm assessment (manual and remote)
- Alarm-response procedures (covering remote- and manual-assessments)
- Incident-reporting procedures
- Local law-enforcement contact and reporting procedures
- Incident-containment procedures
- Key control- and access-procedures
- Procedures for facility access after normal working-hours
- Procedures for sign-out logbook

- Preventative maintenance of the installed equipment
- Arming and disarming sensors
- System-configuration changes
- Placing malfunctioning equipment out-of-service while awaiting repairs
- Testing system's performance

Physical security hardware Upgrades

A normal upgrade package may consist of

- Hardened doors (no glass in them) and high-strength mechanical locks
- Access control systems
- Intrusion-detection and assessment systems
- Balanced magnetic sensors
- Recessed door and window sensors
- Duress switches in device rooms and proximal locations
- Volumetric sensors (motion detectors) in the device room, approach corridors, and exclusion zones
- Tamper-proof connectors (case-hardened, requiring non-standard tools for removal)
- Fiber-optic or other anti-tampering sensors attached directly to the device
- Sirens, alarms and strobe lights
- Alarm enunciation at the Central Alarm Station (CAS)

Employee Training

Employee training is the most difficult aspect of improving security, particularly for training of personnel who develop, design, build, and operate the facility's various specialized radiological equipment. While most employees at medical facilities are trained professionals, their training may center on safety, with little or no emphasis on security. Hence, basic to improving security is having a comprehensive security awareness-training program for these professionals and other personnel having access to devices containing RAM. .

A subset of employee training is ongoing training, response drills, and exercises required for the security response force. This training is provided from both internal- and external- sources. The continued interface with local-law enforcement agencies is vital to a comprehensive response package.

RISK MANAGEMENT AND RISK MITIGATION

The assist-visit team's final report to the appropriate agencies will focus on risks to the devices that contain high-activity sources, as well as to lesser sources used in research, nuclear medicine, radiation oncology, along with recommendations for improvement. Importantly, many of the recommendations will procedural ones, requiring little capital outlay. Recommendations will be prioritized for upgrading security hardware used to mitigate events, affording management the opportunity to appropriately budget less-critical hardware. In many cases, the Department of Homeland Security or Department of Energy may be contacted to provide resources under existing security related programs to support procuring urgent materials or services to mitigate serious existing risks.

The Appendix is a self-audit security checklist. It offers the Director of Security and the RSO a mechanism to jointly assess the progress and effectiveness of the security upgrades. Beginning with a baseline survey, the checklist provides a way to evaluate the contribution of security upgrades to an effective, integrated security-management system.

ORPHAN SOURCES

The Off-Site Source Recovery Project (OSRP) is a U.S. Government activity sponsored by the National Nuclear Security Administration's (NNSA) Office of Global Threat Reduction and is managed at Los Alamos National Laboratory through the Nuclear Nonproliferation Division.

OSRP has the mission to remove excess, unwanted, abandoned, or orphan radioactive sealed sources that pose a potential risk to health, safety, and national security. The initial scope of the Project included any sealed sources comprising Greater than Class C (GTCC) low-level radioactive waste. However, since September 11, 2001, the mission expanded from environmental concerns to address broader public safety and national security requirements.

In addition to transuranic sources, the expanded OSRP mission now includes recovery of beta/gamma emitting sources, which are of concern to both the U.S. government and the International Atomic Energy Agency (IAEA).

Entities having unwanted radioactive sealed sources should register them with OSRP. For registration information, questions, and comments, send e-mail messages to osrp@lanl.gov or call toll-free 877-676-1749.

EXAMPLES OF SECURITY HARDWARE AND SYSTEMS USED TO PROTECT HIGH-ACTIVITY RADIOLOGICAL DEVICES, AND LOW ACTIVITY RADIOACTIVE MATERIAL

This section includes an example list of the proper physical-security hardware for use in security systems for high- and low-activity quantities of radioactive materials that typically are licensed for use in industry, medicine, and research.

Application

The components in the attached tables and the generic room-designs are examples intended for security specialists who review the security of devices, by design engineers who construct security systems for devices, such as a blood irradiator, and by staff responsible for the overall security of the facility, i.e., a hospital complex with installed devices containing RAM. The use of the tables and room-designs below are intended to guide a designer toward a uniform level of security throughout the licensee community. This document includes recommended physical-security hardware components that are appropriate for use in security systems for the types and quantities of radioactive materials typically licensed for use in industry, medicine, and research. The information is provided only as a guide, and is not an endorsement of a particular vendor or product line. Each piece of hardware has specifications on its performance parameters and operating range. A system with comparable performance is an adequate substitute for the equipment named in this document.

The attached tables and room designs provide examples of equipment for

- Intrusion Detection Systems (IDS), for RAM that is at or above the Quantity of Concern
- Access Control Systems (ACS), for RAM below the Quantity of Concern
- Closed Circuit Television (CCTV) Systems

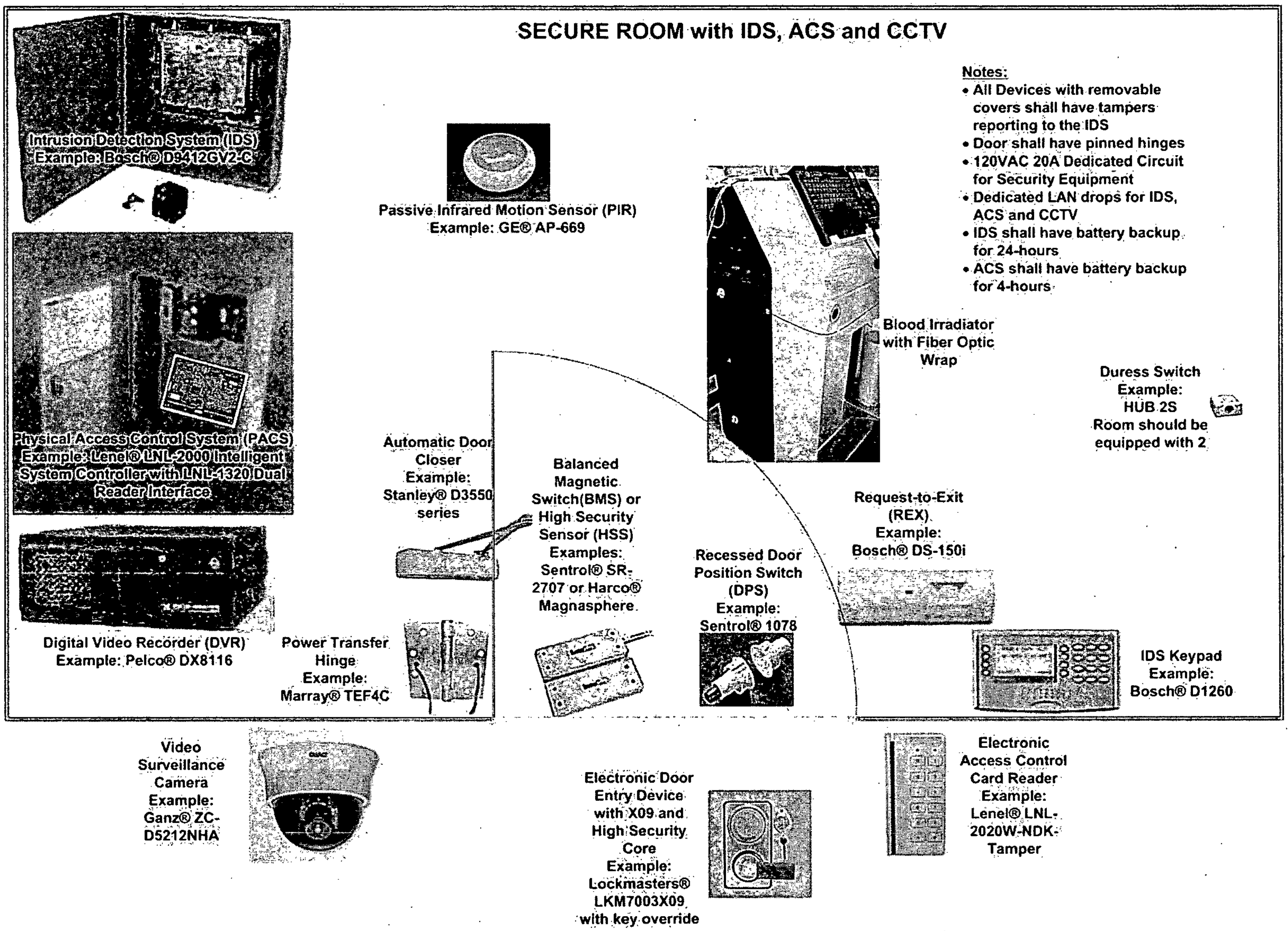
Each category plays a specific role in an integrated security-management system. For the purposes of this paper, those areas that house high activity sources should be equipped with an IDS system that may include ACS and CCTV support. Those areas that house low activity sources can be equipped with an ACS. For RAM that is small in quantity such as those materials found in research laboratory environments, a cipher lock is recommend to avoid the vulnerabilities of key control.

The example equipment listed below offers recommendations; it is not intended to support one vendor over another. Systems incorporating hardware by other vendors are satisfactory, assuming they have equivalent performance specifications. Again, the list is not all encompassing nor is it meant to favor one vendor over another. It serves as an approved starting point to begin designing an integrated security-management system. Cabling, connectors, and races are site-specific, and not included in the list.

INTRUSION DETECTION SYSTEM

The floor plan below incorporates the best features of an intrusion-detection system, access-control system, and a closed-circuit television system that should be used to secure high-activity radiological sources, such as devices used to diagnose and treat cancer patients or other industrial type irradiators.

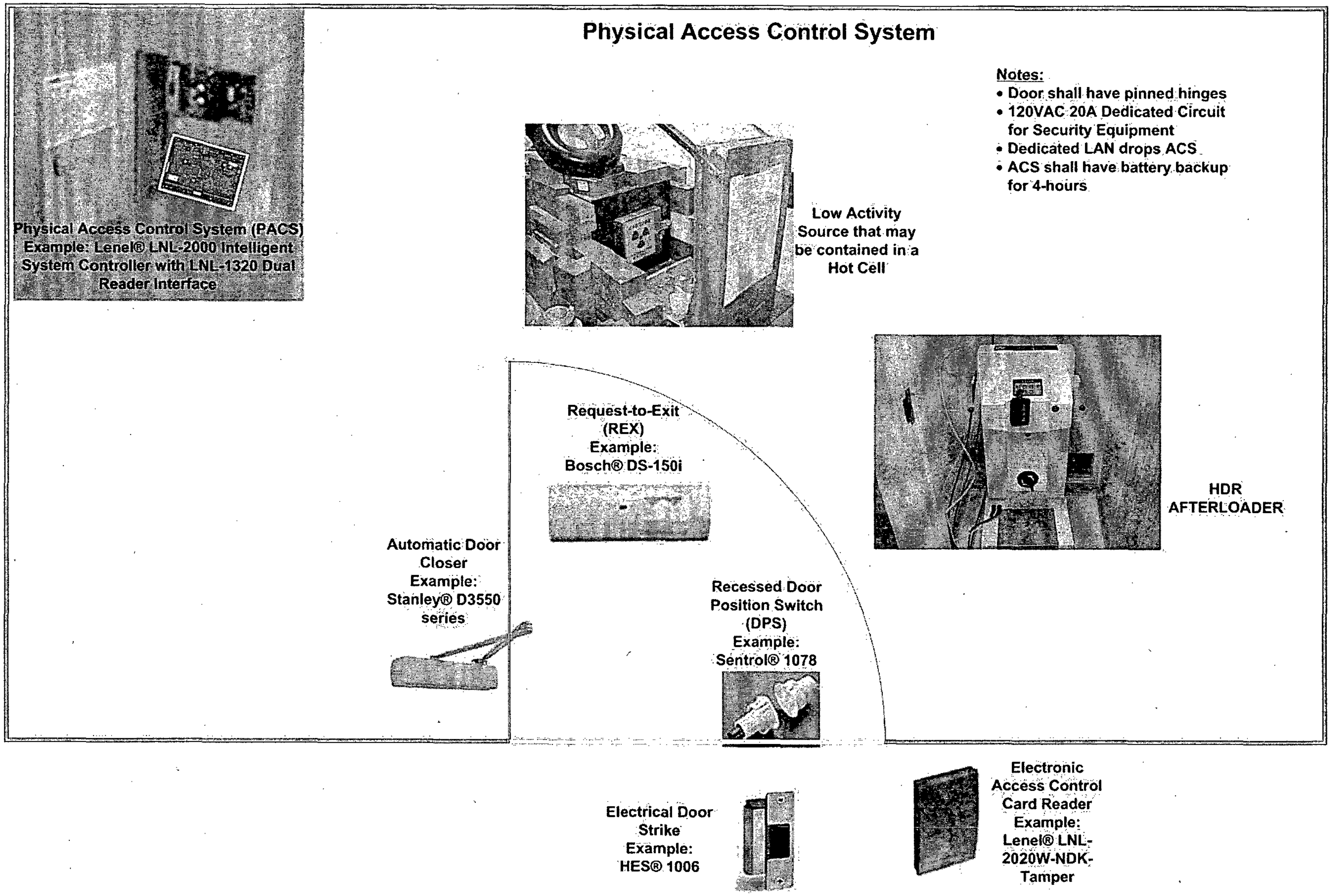
IDS General IGCE				
Item	**Quantity**	**Description**	**Cost ($/Unit)**	**Total ($)**
1	1	Bosch D9412GV2-C	800	800
2	1	Bosch D110 Tamper	100	100
3	1	Bosch DX4020	300	300
4	1	Bosch Battery (24Hr)	200.	200
5	1	Bosch D1260 Keypad	300	300
6	1	AP669 or Sharp-Shooter	150	150
7	1	Sentrol 2707 BMS	220	220
8	1	Misc. Equipment (e.g., cable, conduit, warranty, LAN Adjustable Cost	2,000	2,000
9	1	HUB S2 Duress Switch	$50.00	$50.00
10	80	Integrator Hours (Technicians, PM, Programming, Engineering)	95	7,600
			SUBTOTAL	11,720
		General Contractor/GSA Markup - Minimum 20%	1.20	
			TOTAL	**14,064**


SECURE ROOM with IDS, ACS and CCTV
Notes:
• All Devices with removable covers shall have tampers reporting to the IDS
• Door shall have pinned hinges
• 120VAC 20A Dedicated Circuit for Security Equipment
• Dedicated LAN drops for IDS, ACS and CCTV
• IDS shall have battery backup for 24-hours
• ACS shall have battery backup for 4-hours
Intrusion Detection System (IDS) Example: Bosch® D9412GV2-C
Passive Infrared Motion Sensor (PIR) Example: GE® AP-669
Blood Irradiator with Fiber Optic Wrap
Duress Switch Example: HUB 2S Room should be equipped with 2
Physical Access Control System (PACS) Example: Lenel® LNL-2000 Intelligent System Controller with LNL-1320 Dual Reader Interface
Automatic Door Closer Example: Stanley® D3550 series
Balanced Magnetic Switch(BMS) or High Security Sensor (HSS) Examples: Sentrol® SR-2707 or Harco® Magnasphere
Recessed Door Position Switch (DPS) Example: Sentrol® 1078
Request-to-Exit (REX) Example: Bosch® DS-150i
Digital Video Recorder (DVR) Example: Pelco® DX8116
Power Transfer Hinge Example: Marray® TEF4C
IDS Keypad Example: Bosch® D1260
Video Surveillance Camera Example: Ganz® ZC-D5212NHA
Electronic Door Entry Device with X09 and High Security Core Example: Lockmasters® LKM7003X09 with key override
Electronic Access Control Card Reader Example: Lenel® LNL-2020W-NDK-Tamper

ACCESS CONTROL SYSTEM

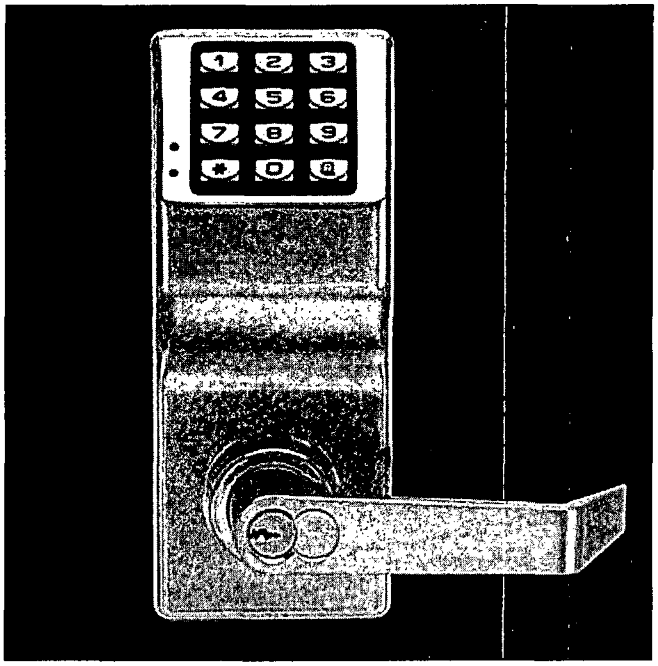
The floor plan below incorporates the best features of an Access Control System that should be used to secure low-activity radiological sources, i.e., nuclear-medicine hot cells, waste and storage of low-activity treatment sources, and research laboratory-grade sources…

Access Control System General IGCE				
Item	**Quantity**	**Description**	**Cost ($/Unit)**	**Total ($)**
1	1	Lenel® LNL-1320 – Dual Card Reader Interface	700	700
2	1	Mercury® BR-20 – Magswipe Card Reader with Indestructible Keypad and tamper	750	750
3	1	HES 1006 (mortise)	500	500
4	1	Automatic Door Closer	350	350
5	1	Bosch DS-150i	100.	100.
6	1	Sentrol SR-1078	20.	20.
7	1	Store Room Function Mortise Locks - Medeco IC Grade 1 Ready	300	300
8	1	Medeco IC Core (all doors, pinned and keyed)	155	155
9	1	Misc. Equipment (e.g., cable, conduit, warranty) Adjustable Cost	500	500
10	16	Integrator Hours (Technicians, PM, Engineering)	95	1,520
			SUBTOTAL	4,895
		General Contractor/GSA Markup - Minimum 20%	1.20	
			TOTAL	**5,874**


Physical Access Control System
Notes:
• Door shall have pinned hinges
• 120VAC 20A Dedicated Circuit for Security Equipment
• Dedicated LAN drops ACS
• ACS shall have battery backup for 4-hours
Physical Access Control System (PACS) Example: Lenel® LNL-2000 Intelligent System Controller with LNL-1320 Dual Reader Interface
Low Activity Source that may be contained in a Hot Cell
Request-to-Exit (REX) Example: Bosch® DS-150i
HDR AFTERLOADER
Automatic Door Closer Example: Stanley® D3550 series
Recessed Door Position Switch (DPS) Example: Sentrol® 1078
Electrical Door Strike Example: HES® 1006
Electronic Access Control Card Reader Example: Lenel® LNL-2020W-NDK-Tamper

Recommended Security Upgrade for Simple Door Locks

For low risk areas that do not require and Intrusion Detection System or and Access control System.



Recommended Security Upgrade Equipment List

Access Control System	
Item	**Cost ($/Unit)**
Lenel® LNL-2000 Intelligent System Controller	1,567
Lenel® LNL-1000 Intelligent System Controller	800
Lenel® LNL-ETHLAN-MICR Ethernet Adaptor	192
Lenel® LNL-1320 – Dual Card Reader Interface	600
Lenel® LNL-1300 - Single Card Reader Interface	250
Lenel® LNL-MSS Ethernet Adaptor	275
Lenel® LNL-1007MK - 7 MB of memory	660
Mercury® BR-20 – Magswipe Card Reader with Indestructible Keypad	700
Lenel® LNL-2020W	300
Lenel® LNL-2010W	190
Sagem Morpho MA120W Smart Card Reader	595
BridgePoint FIPS-201 Edge Reader	650
Lenel Enterprise Redundant Server - NEC® 5800/320Lc	40,000
Lenel Client Workstation	3,000
Badge Printer	7,000
Lenel Enterprise Annual Support Agreement	25,000
HES 1006	300
HES 5000	125
HES 9600	400
HES 7000	300
Door Closer	100
Bosch DS-150i	100
Sentrol 1078	5
Continuous Astragal	400
Flush Bolts for Inactive Leaf - S&G #181	50
Lenel® LNL-AL400ULX – Altronix® 4AMP Power Supply	450
Lenel® ABT-12 – Battery Kit and Battery	69
HIRSH DS47L Scramble Pin pad and mounting box (MB-2)	285
Schlage LC-SERIIIWS Scramble Pin Pad	767.99
Xico 3892SD Card Reader	168

IDS	
Bosch D950 50'X50' PIR/MICROWAVE TRITECH	56
Bosch D7412G	325
Bosch D110 Tamper	20
Bosch DX4020	250
Bosch Battery (24Hr)	200
Bosch 1260 Keypad	200
AP669 or SharpShooter	125
SENTROL 2707ADL HIGH SECURITY CONTACTS	141
Glassbreak Sensor	100
Bosch ® D6680-E120 Network Interface Cards	850
Bosch ® D6600 Alarm Receiver	5,500
Duress Button	30
Optex VX-402 Dual Tech	139
OD850F1 Outdoor Tritech Motion Detector	104.95
CCTV	
ICS-150 (Low Light, High Res)	430
AD Intellex DVR	10,000
Pelco DX8016 - 1.2TB	10,0000
Pelco Spectra 3	3,000
CCTV Power supply	350
Pelco ® 9760 - MDA	1,300
Dedicated Micros DS2 DVR	3,900
Panasonic DVR WJ-HD316A/1000V	5,000
SPECO CVC-7706DNV Bullet Camera with IR	399
SPECO HT-7915DNV 5 - 50mm Bullet Camera with IR	415
Axis 241Q IP Video Server	800
4XEM EVS400 Enterprise Quad	700
NVT NV-653T Transmitter	173
NVT NV-1662R Hub	2,636
GE S704VTEST Fiber Video Transceiver	1,100
NVT NV-652R Receiver	173

Control and Display Equipment	
Pelco 17" with quad	600
Tripplite 16-port KVM w/ 15" LCD	2,500
Avocent 4-port KVM	400
Avocent 2-port KVM	150
Communications	
Cisco 3550 24-port Switch	3,500
AFI RR-404C	1,100
AFI MT-404C	1,100
AFI RR-404	1,200
AFI MT-404	1,200
AFI RRM-1420	1,100
AFI MTM-1420	1,100
AFI PSR2 with 19" rack	800
AFI RR-10	400
AFI RT-10	400
AFI RX-45-FX-ST	1,100
AFI RRM-30	700
AFT MTM-30	700
IFS 7130 Data Transceiver	1,400
IFS PS-12VDC-R3 Power Supply	800
Allied Telesyn MC-101 (10/100 Ethernet)	200
Door Hardware	
Store Room Function Mortise Locks - Medeco IC Grade 1 Ready	300
Store Room Function Electrified Mortise Locks - Medeco IC Grade 1 Ready	650
Store Room Function Cylindrical Levers - Medeco IC Grade 1 Ready	300
Store Room Function Electrified Cylindrical Levers - Medeco IC Grade 1 Ready	650
Door Cylinder Blanks and misc. parts	150
Von Duprin 98/99 Crash Bars with REX	1,000
Von Duprin 98/99 Crash Bars with Rods/REX	1,500
Von Duprin 33A/35A Crash Bar with Rods/REX	1,500
Von Duprin PS873	450
Von Duprin EPT-10 Transfer Hinge	250
Medico IC Core (all doors, pinned and keyed)	95

Latch Protector	50
Armored Door Cord	50
Locks	
KABA MAS CDX-09 High Security Locks	2,000
Adams Rite 7440 Electric Strike	120
BEST IDH MAX 1300 Mortise Lock with integrated reader	800
Trilogy Lock T2 DL270	368
Misc.	
Lights - Edwards 104FLDR-G1, 24DC	150
20A 120VAC Circuits from TK Services (front doors, LAN room, loading dock)	2,000
TK Services cost to ADD a DOOR	5,000
Mag-Lock Fire Drop	2,000
Fiber - 12 Strand	7,500
Misc. Equipment (cable, conduit, and the like)	25,000
Integrator Hours (Technicians, PM, Engineering)	75

ABBREVIATIONS

Access Control System	ACS
Brookhaven National Laboratory	BNL
Central Alarm Station	CAS
Closed Circuit Television	CCTV
Department of Health and Mental Hygiene	DOHMH
Increased Controls	IC
Intrusion Detection System	IDS
Nuclear Regulatory Commission	NRC
Office of Radiological Health	ORH
Radiation Safety Officer	RSO
Radioactive Materials	RAM
Radiological Dispersion Device	RDD

APPENDIX

Security Self-Audit Checklist

SECURITY SELF-AUDIT CHECKLIST

Section #1 High-Activity Devices

	QUESTION	Yes-No-N/A	ADDITIONAL REMARKS
1	Are the devices located in an exclusion zone?	☐ ☐ ☐	
2	Are the devices located in a single use room?	☐ ☐ ☐	
3	Are the sources secured behind hardened doors and mechanical locks?	☐ ☐ ☐	
4	Are there any additional sensors or alarms on the door?	☐ ☐ ☐	
5	Are there any CCTV cameras in the exclusion zone?	☐ ☐ ☐	
6	Are keys secured in a lock box with sign out logs?	☐ ☐ ☐	
7	Is there a direct line of communications to security?	☐ ☐ ☐	
8	Is there more than one entrance into the exclusion zone?	☐ ☐ ☐	
9	Is there an authorized access list posted?	☐ ☐ ☐	
10	Are the personnel in the device area properly trained regarding security	☐ ☐ ☐	Describe

***Additional comments, remarks, recommended rapid upgrades ***

SECURITY SELF-AUDIT CHECKLIST

Section # 2 Area Security

	QUESTION	Yes-No-N/A	ADDITIONAL REMARKS
1.	Is access through the gate/gates controlled?	☐ ☐ ☐	
2.	Do the gates lock or can they remain secured?	☐ ☐ ☐	
3.	Are they manually controlled or electrically controlled or both?	☐ ☐ ☐	
4.	What times of the day/week are the gates locked?	Describe	
5.	Are there any counter ram devices?	☐ ☐ ☐	
6.	What is the distance between the exterior and interior fences?	Describe	
7.	What is the inner fence made of?	☐ ☐ ☐	
8.	Are there any Intrusion Detection Systems within this protective space?	☐ ☐ ☐	
9.	Is this area monitored in any manner?	☐ ☐ ☐	
10.	Is this area patrolled?	☐ ☐ ☐	

*** **Additional comments, remarks, recommended rapid upgrades** ***

OFFICIAL USE ONLY

(When filled out)

SECURITY SELF-AUDIT CHECKLIST

Section #3 CCTV

	QUESTION	Yes-No-N/A	ADDITIONAL REMARKS
1	Does the facility have a CCTV system?	☐ ☐ ☐	
2	Does it operate effectively in lighting, weather and temperature extremes?	☐ ☐ ☐	
3	Do the cameras cover the entire facility?	☐ ☐ ☐	
4	Do the cameras overlap in their coverage areas?	☐ ☐ ☐	
5	Do they have hardened power supplies?	☐ ☐ ☐	
6	Are they able to remotely Pan, Tilt and Zoom?	☐ ☐ ☐	
7	Can the facility record from the cameras?	☐ ☐ ☐	
8	How often must they change out tapes?	☐ ☐ ☐	Describe
9	How long do the tapes record for?	Describe	
10	Is the CCTV system a discreet or visible deterrent?	☐ ☐ ☐	

*** **Additional comments, remarks, recommended rapid upgrades** ***

OFFICIAL USE ONLY

(When filled out)

Section # 4 Intrusion Detection System(s)

	QUESTION	Yes-No-N/A	ADDITIONAL REMARKS
1	What type of Intrusion Detection System does the facility have?	Describe	
2	Is it audible, passive or both?	☐ ☐ ☐	
3	Are there periodic false alarms? Are these false alarmed assessed?	☐ ☐ ☐	
4	Is coverage only on the device room or are other areas included?	☐ ☐ ☐	
5	Is there a backup power system for the system?	☐ ☐ ☐	
6	Are the systems periodically tested and the results recorded?	☐ ☐ ☐	
7	Who does the system alert if an alarm is triggered?	Describe	
8	Has there ever been a reported breech of the IDS?	☐ ☐ ☐	
9	Has the system ever been physically tested from within?	☐ ☐ ☐	
10	If there were deficiencies, were they corrected?	☐ ☐ ☐	

***** Additional comments, remarks, recommended rapid upgrades *****

SECURITY SELF-AUDIT CHECKLIST

Section #5 Support Buildings and Structures

	QUESTION	Yes-No-N/A	ADDITIONAL REMARKS
1	Are the facility's buildings located behind a security fence?	☐ ☐ ☐	
2	Are the doors and windows protected in any special manner?	Bars, Screens, Metal vs. wood	
3	How is access to the building controlled?	☐ ☐ ☐	
4	Is there a janitorial service on site for all of the buildings?	☐ ☐ ☐	
5	How are the personnel selected?	☐ ☐ ☐	
6	How is the facility's trash disposed of?	☐ ☐ ☐	
7	How are the day-to-day deliveries to the facility controlled?	☐ ☐ ☐	
8	Does the facility have a protocol for visitors?	☐ ☐ ☐	Official, Educational?
9	Is there a parking lot for employees?	☐ ☐ ☐	
10	If so is it secured?	☐ ☐ ☐	
11	Does management have selected parking areas?	☐ ☐ ☐	Are they marked?
12	Is the Central Alarm Station (CAS) located in a security area?	☐ ☐ ☐	
13	What is the CAS constructed of?	How many floors, entrance doors?	
14	Is there adequate security for the CAS?	☐ ☐ ☐	Inside and out?

OFFICIAL USE ONLY
(When filled out)

SECURITY SELF-AUDIT CHECKLIST

15	How is access into the CAS controlled?	Describe	
16	Are hard line phone wires in and out readily accessible?	☐ ☐ ☐	Explain
17	Are ventilation, A/C and heating ducts accessible?	☐ ☐ ☐	Explain
18	Is the CAS monitoring protected by anything?	☐ ☐ ☐	Explain - (i.e. bullet proof glass, steel doors, .)
19	How many CAS personnel are on each shift?	Describe	
20	Is there a response Force?	☐ ☐ ☐	
21	Is the response force properly trained and equipped?	☐ ☐ ☐	
22	Do they conduct roving patrols?	☐ ☐ ☐	Explain – (i.e. showers, kitchen, dining area)
23	Are the patrols on a fixed schedule or random?	Describe	
24	Is there an effective working relationship with local law enforcement?	☐ ☐ ☐	
25	Are there coordinated exercises with local law enforcement agencies?	☐ ☐ ☐	Explain

*** Additional comments, remarks, recommended rapid upgrades ***

SECURITY SELF-AUDIT CHECKLIST

Section # 6 Material Storage facilities

	QUESTION	Yes-No-N/A	ADDITIONAL REMARKS
1	How many material storage structures are at the site?	Explain	
2	Are they above ground, below ground or both?	Explain	
3	What material is the above ground structure made of and diemsions?	Describe	
4	Are these structures behind security fences and or gates?	☐ ☐ ☐	How many?
5	Are the material storage structures regularly patrolled?	☐ ☐ ☐	By whom and by what means?
6	What is the foundation's composition?	Explain – (i.e. dirt, cement, wood, asphalt,)	
7	Is the foundation secure from a tunneling?	☐ ☐ ☐	Explain
8	Are the structures walls secure from a tunneling?	☐ ☐ ☐	
9	Are there any vents or ducting that may be accessible?	☐ ☐ ☐	Explain (how large are the openings?) Are the openings grated?
10	Are there windows and doors to the structure?	☐ ☐ ☐	Explain and describe locations
11	Are the exterior doors alarmed?	☐ ☐ ☐	Explain
12	Are the windows alarmed? If not are the windows grated?	☐ ☐ ☐	Explain
13	Are there any motion detectors on the inside of the structures?	☐ ☐ ☐	
14	Are there any trees, bushes or other vegetations close by?	☐ ☐ ☐	Does it offer access to the roof or concealment?

OFFICIAL USE ONLY

(When filled out)

SECURITY SELF-AUDIT CHECKLIST

15	Is there material stacked close by the buildings?	☐ ☐ ☐	Does it offer access to the roof or concealment?
16	Is the use of electrical hoist equipment controlled?	☐ ☐ ☐	Explain
17	Are there underground storage facilities on the site?	☐ ☐ ☐	
18	Are the U/G storage facilities secured?	☐ ☐ ☐	Describe
19	Are the U/G storage facilities alarmed?	☐ ☐ ☐	Describe
20	Are the U/G storage facilities patrolled?	☐ ☐ ☐	By whom and by what means?
21	How is access to the U/G storage facilities controlled?	☐ ☐ ☐	Describe
22	Are there radiation monitors in the facility?	☐ ☐ ☐	
23	How are the U/G vault lids removed?	Describe	
24	What is the dimension and weight of each vault lid?	Describe	
25	Can the vault lids be removed by other means not originally intended? i.e. pried off, dragged away by vehicle, etc..	☐ ☐ ☐	

*** Additional comments, remarks, recommended rapid upgrades ***

OFFICIAL USE ONLY

(When filled out)

SECURITY SELF-AUDIT CHECKLIST

Section # 7 Communications

	QUESTION	Yes-No-N/A	ADDITIONAL REMARKS
1	Does the facility have adequate telephone communications?	☐ ☐ ☐	
2	Are the hard lines coming into the facility protected?	☐ ☐ ☐	Describe
3	Are telephone calls routed at the facility (i.e.; a switchboard)	☐ ☐ ☐	
4	Can telephone calls (in/out) be monitored by the facility?	☐ ☐ ☐	Describe
5	Is there an emergency procedure if telephone service is severed?	☐ ☐ ☐	Describe
6	Does facility have a radio communication system?	☐ ☐ ☐	
7	Can the facility communicate with local authorities by radio?	☐ ☐ ☐	List
8	Does each on duty member of the security force have a portable radio?	☐ ☐ ☐	
9	Do the portable radios have multiple radio channels?	☐ ☐ ☐	How many?
10	How many frequencies does the facility use and frequency compatibility with LLEA and potential responders?	Describe	

*** **Additional comments, remarks, recommended rapid upgrades** ***

OFFICIAL USE ONLY

(When filled out)

SECURITY SELF-AUDIT CHECKLIST

Section # 8 Area Security

	QUESTION	Yes-No-N/A	ADDITIONAL REMARKS
1	Are there adjacent roadways near the facility?	☐ ☐ ☐	
2	Are background checks performed on the company/employees?	☐ ☐ ☐	
3	Are the vehicles searched both before entry and again before exit from the site??	☐ ☐ ☐	
4	Is the entry/exit station inside or outside of perimeter fencing?	☐ ☐ ☐	
5	Is this location secured?	☐ ☐ ☐	
6	Are there employee-parking areas	☐ ☐ ☐	
7	Are the parking areas fenced?	☐ ☐ ☐	
8	Are the lots patrolled or monitored by some other source?	☐ ☐ ☐	
9	Are there any special controls for parking in these areas (I.D.)?	☐ ☐ ☐	
10	Are there random vehicle checks	☐ ☐ ☐	

*** **Additional comments, remarks, recommended rapid upgrades** ***

OFFICIAL USE ONLY

(When filled out)

SECURITY SELF-AUDIT CHECKLIST

Section # 9 Identification of personnel and vehicles

	QUESTION	Yes-No-N/A	ADDITIONAL REMARKS
1	Do security personnel request positive proof of all persons who enter and leave the facility?	☐ ☐ ☐	
2	Do executives park in marked areas that identify who they are? (Doctors, nurses, technicians?)	☐ ☐ ☐	
3	Is there an ID system for employees, visitors or contractors?	☐ ☐ ☐	
4	Are the ID cards color-coded and visually readily distinguishable at a distance for security purposes?	☐ ☐ ☐	
5	Is there a package pass system for deliveries or refuse hauling?	☐ ☐ ☐	
6	Are employee entrances/exits controlled?	☐ ☐ ☐	
7	Are visitors and contractors logged in and out?	☐ ☐ ☐	
8	Are delivery drivers monitored while their cargo is off loaded? Do vendors and service providers certify the backgrounds of their delivery or service personnel?	☐ ☐ ☐	
9	Is there a waiting area or lounge for the drivers?	☐ ☐ ☐	
10	Is there a central delivery area where radiological safety of delivered packages is verified and custody is transferred from vendor to facility personnel?	☐ ☐ ☐	

***** Additional comments, remarks, recommended rapid upgrades *****

OFFICIAL USE ONLY

(When filled out)

SECURITY SELF-AUDIT CHECKLIST

Section # 10 Key and Key Access Control

	QUESTION	Yes-No-N/A	ADDITIONAL REMARKS
1	Who has control of and authority to issue keys?	Describe	
2	Are physical inventories of keys made?	☐ ☐ ☐	How often and by whom?
3	Are there master keys and/or grand master keys issued to anyone?	☐ ☐ ☐	
4	How are the keys to different locations identified?	Describe	
5	Are locks changed periodically as a pro-active deterrence?	☐ ☐ ☐	
6	Is there a strict accountability system for key control?	☐ ☐ ☐	
7	Is there a list of authorized persons to use/check out keys?	☐ ☐ ☐	
8	Do they have sample signatures on file?	☐ ☐ ☐	
9	Is there a master or grand master key box?	☐ ☐ ☐	
10	How is this box secured and who has access to it?	Describe	
11	Is the type of key covered by an agreement with licensed locksmiths regarding unauthorized duplication?	☐ ☐ ☐	

*** **Additional comments, remarks, recommended rapid upgrades** ***

OFFICIAL USE ONLY
(When filled out)

SECURITY SELF-AUDIT CHECKLIST

Section #11 Response Forces

	QUESTION	Yes-No-N/A	ADDITIONAL REMARKS
1	How are Pro-Force personnel selected?	Describe	
2	Are background checks & interviews conducted?	☐ ☐ ☐	
3	Are their wages adequate for their training and duties?	☐ ☐ ☐	
4	Is there a physical fitness requirement for employment?	☐ ☐ ☐	
5	Is there a physical fitness requirement for continued employment?	☐ ☐ ☐	
6	Number of personnel assigned to security force at the site?	Describe	
7	Of the total number of security personnel, how many are management?	Describe	
8	Do management personnel work shifts?	☐ ☐ ☐	What are their hours?
9	What hours of the day do the shifts cover for the field force?	Explain day and hour coverage	
10	How many personnel are on duty on each shift?	Describe	
11	How many breaks does the field force take per shift?	Is more than one person on break at a time?	
12	Where are their breaks taken?	Break room, lunchroom or restaurant?	
13	Are friends and/or family allowed to take breaks with them?	☐ ☐ ☐	
14	Are personnel allowed to leave the facility while on breaks?	☐ ☐ ☐	
15	Are friends and/or family allowed to visit the site?	☐ ☐ ☐	While personnel are on duty?
16	Are security personnel properly equipped?	☐ ☐ ☐	

OFFICIAL USE ONLY
(When filled out)

SECURITY SELF-AUDIT CHECKLIST

17	Are the security personnel armed?	☐ ☐ ☐	Describe weapons systems
18	If so, what is their level of firearms training? Specify levels so they can select one?	Describe	
19	Is continuing training offered to security personnel?	☐ ☐ ☐	Describe
20	Are the weapons systems secured on the facility?	☐ ☐ ☐	
21	Do other non security personnel have access to them?	☐ ☐ ☐	
22	How do the security personnel report incidents?	Describe	
23	Are there any documented incidents of intrusion, vandalism or theft on file?	☐ ☐ ☐	
24	Do the shifts inner act with information?	☐ ☐ ☐	
25	Are there procedures for security operations during nights, weekends, and holidays? During periods of non-standard (emergency) operations?	☐ ☐ ☐	
26.	What are post orders regarding radiological threats, rules of engagement relative to facility-identified threat scenarios, policy regarding use of potentially lethal force?	Describe	

***** Additional comments, remarks, recommended rapid upgrades *****

OFFICIAL USE ONLY

(When filled out)

SECURITY SELF-AUDIT CHECKLIST

Section # 12 Documents, Training & Procedures

	QUESTION	Yes-No-N/A	ADDITIONAL REMARKS
1	Verify there is no sensitive information on public accessible websites	☐ ☐ ☐	
2	Is there an existing Security Assessment?	☐ ☐ ☐	
3	Is there an existing document that describes the "Threat"	☐ ☐ ☐	
4	Are there any committees to discuss vulnerabilities and threats?	☐ ☐ ☐	
5	Is there a formal Training Department?	☐ ☐ ☐	
6	Does the response force receive formal training?	☐ ☐ ☐	
7	Is firearm qualification part of the training program?	☐ ☐ ☐	
8	Any special equipment training provided to the security personnel?	☐ ☐ ☐	
9	What is the basis for promotion in the security personnel?	Describe	
10	Is there a formal Procedures Department?	☐ ☐ ☐	
11	Does security provide its own procedures?	☐ ☐ ☐	
12	Do written procedures exist?	☐ ☐ ☐	
13	Does the security force have access to computers?	☐ ☐ ☐	
14	Are there training films available?	☐ ☐ ☐	
15	Are shift logs kept?	☐ ☐ ☐	

OFFICIAL USE ONLY
(When filled out)

SECURITY SELF-AUDIT CHECKLIST

16	Are offsite classes and/or training available to security personnel?	☐ ☐ ☐	
17	Are security equipment maintenance logs kept?	☐ ☐ ☐	
18	Do security personnel perform other duties	Describe	
19	Do facilities exist for Training?	☐ ☐ ☐	
20	Annual or periodic training or recertification frequency?	Describe	

*** **Additional comments, remarks, recommended rapid upgrades** ***

OFFICIAL USE ONLY

(When filled out)

EDITORIAL

Cesium Chloride: Dispersibility or Security?

Stephen V. Musolino*, D. Thomas Coulter†, Hailu Tedla‡

The National Academy of Sciences 2008 study evaluated technologies and made recommendations for replacing existing high-activity radioactive materials that could be used for malevolent purposes. Their report recognized the possibility for substituting this material with non-radionuclide alternatives, and of developing new technologies: the authors expressed greater concern about cesium chloride, including proposing discontinuing its licensing and usage. They also recommended caution in implementing alternatives to ensure the preservation of original material's essential functions (NAS 2008).

The widespread use of cesium chloride is a vital component of radiobiological- and medical-research, and of clinical medicine, so that any decision to eliminate its use has far-reaching implications in these fields. Currently, and for the near future, there is no alternative to it in many applications. The ^{137}Cs monoenergetic spectrum has been the reference standard for radiobiological research for over 60 years and is the basis for national- and international-standards for dosimetry and instrument calibration; it cannot simply be replaced by x-rays. Indeed, any move away from using the ^{137}Cs spectrum

* Brookhaven National Laboratory, Nonproliferation and National Security Department, P.O. Box 5000, Upton, NY 11973-5000

† New York City Department of Health and Mental Hygiene, 2 Lafayette Street, 11th Floor, New York, NY 10007

‡ PHROBUS, Inc, 2428 Sterling Point Drive, Portsmouth, VA 23703

would necessitate years of repetition of impractical and fundamental radiobiological studies to redefine and verify another standard. Its outright elimination would impose great difficulties and financial hardship on clinical-medical applications. While there are viable alternatives for some procedures that are not spectrum-dependant, such as blood irradiation, the use of accelerators and x-ray machines is expensive, much less reliable, and their maintenance is very costly. Furthermore, most operators do not want these machines in hospitals where space is at a premium because they typically encompass to three times more space to accommodate their chillers and associated equipment.

It is commonly known from reports of the intelligence community that terrorist groups have expressed their interest to carry out radiological terrorism. To deal with this threat, the Nuclear Regulatory Commission (NRC) issued an Emergency Order in 2005 that required Increased Controls to upgrade the security of high-activity sources of radioactive materials, Table 1 (NRC 2005). Subsequently, licensees nationwide implemented these requirements, thereby vastly reducing the risk of diversion to a malevolent purpose.

So what would happen if a terrorist incident with radioactive material occurred? The dispersal pattern inevitably will be a function of the following parameters (Harper et al 2007):

- The design of the device
- The quantity of the material
- The material's chemical- and physical-form, e.g., soluble, insoluble, powder, ceramic, or metal
- The resulting aerosol fraction and the particle size distribution

These issues are fully applicable to cesium chloride, and for all other high-activity radioactive materials that are manufactured and distributed worldwide specifically for industrial-, medical-, and research-purposes.

Cesium chloride is a soluble powder. Hence, one solution to reducing the risk of its dispersal is to re-engineer it into an insoluble, solid matrix, such as glass or the zeolite mineral pollucite. However, while the changeover to more refractory form is desirable, for various reasons, it may not be an entirely successful means of mitigating the terrorist threat:

1. Research is needed to develop a method to identify and manufacture an alternative form offering comparable specific activity in the matrix. Currently, cesium chloride is produced with approximately 70% ^{137}Cs. The United States does not have internal capability to do such research, the cost of funding the research may be prohibitive, and there is risk that the outcome will not be satisfactory.
2. Any substitute form generated with similar specific activity in the matrix must have a similarly sized volume. Lacking that, the manufacturers and equipment owners face major, expensive re-engineering of the irradiator itself, or even its complete replacement.
3. Should a less dispersible form eventually be developed, this achievement still does not negate completely the risk of malevolent use, and the subsequent large cleanup and economic costs of recovery.

If we assume, with these constrains, that the Increased Controls vastly lowered the risk of diversion of cesium chloride, we still must consider whether a creditable deterrence was put in place to discourage any terrorist's acquisition of cesium chloride (or other regulated high-activity radioactive materials). Is there a residual risk still that justifies its elimination? Is there any quantitative evidence of any significant residual risk? We consider that the answer is "no" because the residual risk for cesium chloride is a part of a myriad of possible terrorist acts with and without radioactive material that can harm people or lead to large-scale impacts on society. Cesium chloride is just one component of this continuum of threats, and hence, decisions on its fate should be made within this context. We also believe that its replacement is not needed because the Increased Controls successfully lowered the risk of material diversion. Credit should be taken for the improvements to security of all high-activity sources and the resulting deterrent to criminal diversion and malevolent use. In addition, there are empirical data to justify the risk reduction.

The New York City Department of Health and Mental Hygiene in 2006 and 2008, and the Department of Homeland Security in 2006 contracted Brookhaven National Laboratory to conduct non-regulatory assist visits to licensee sites. The objective was to share security best practices and offer advice on opportunities for improvement. Because all the licensees with high-activity sources were inspected previously, and approved as complying with the Increased Controls, the visits complemented regulatory requirements, but did not conflict with them. Eventually, 94 individual visits were completed; we assisted 14 licensees with ^{137}Cs irradiators located in Connecticut, New Jersey and in areas of New York beyond the boundaries of New York City, and 80 licensee sites within New York City. Not all of the latter contained high-activity sources; in that context, New

York City officials took a holistic approach to all quantities of radioactive materials used by their licensees.[§]

The overall results from the 94 reviews clearly demonstrated that despite the success of the Increased Controls, the team was able to make meaningful recommendations for improving security, invariably at little cost to the licensee; they covered enhancements in physical-security hardware, and administrative policies and procedures (Musolino and Coulter 2009).

An intangible beneficial impact of the assist visits was our team's emphasis on maintaining the security awareness of the facilities' management and operators. We emphasized close cooperation between the Radiation Safety Officer and the facility's Security Manager, and encouraged a strong working relationship with the staff of the local police precinct. We promoted security training for all levels of the workforce, and tabletop exercises for management to evaluate in-place policies and procedures. Within New York City, a representative from the Department of Health and Mental Hygiene Bureau of Environmental Emergency Preparedness and Response joined the assist visit team; occasionally, a representative from New York Police Department Counterterrorism Bureau accompanied us[**]. Outside New York City, a representative from the local law-enforcement agency joined the review, along with an agent from the regulatory authorities, viz., the Nuclear Regulatory Commission in Connecticut and New Jersey, and the Department of Health in New York State. Invariably, their presence enhanced the overall assist visit, as was particularly noticeable when encouraging a strong working

[§] The Department of Health and Mental Hygiene is the licensing authority for radioactive material used for medical, academic, and research purposes in New York City.

[**] The NYPD Counter Terrorism Bureau routinely visits the licensees and maintains an ongoing relationship for security.

relationship with the local police precinct. We cannot overstate the value of the presence of a representative from the local law enforcement agency that would respond to the facility in an emergency to interdict an attempted theft of radioactive material.

CONCLUSIONS

- Changing cesium chloride to a different physical form does not eliminate the potential for a malevolent dispersal; re-engineering the physical form will be costly, and its success debatable.
- Any of the proposed alternatives to cesium chloride most likely will impose a significant economic impact, and present other serious drawbacks for clinical medicine and medical research.
- The institution of the Increased Controls mitigated the risk of cesium chloride so that its risk is only one of a continuum of terrorist threats. Although its potential impacts were not eliminated, the residual risk of this material is acceptable (or close to it), and proven opportunities exist for cost-effective improvements to security.

Notice: The opinions expressed in this editorial are those of the authors and do not represent the official opinion or position of the Brookhaven National Laboratory, National Laboratories, the U.S. Department of Energy, or the New York City Department of Health and Mental Hygiene. This manuscript has been authored by Brookhaven Science Associates, LLC under Contract No. DE-AC02-98CH1-886 with the U.S. Department of Energy. The United States Government retains, and the publisher, by accepting the article for publication, acknowledges, a worldwide license to publish or

Acknowledgments — Funding for the security reviews was provided by the Department of Homeland Security Domestic Nuclear Detection Office and from New York City Department of Health and Mental Hygiene Bureau of Environmental Emergency Preparedness and Response through grants received from the Department of Homeland Security and the Centers for Disease Control. We greatly appreciate the technical writing expertise of Avril Woodhead.

References

Harper, F.T., Musolino, S.V. And Wente, W.B.. Realistic radiological dispersal device hazard boundaries and ramifications for early consequence management decisions, Health Physics 93:1-16; 2007.

Musolino, S.V. and Coulter, D.T. Best practices for securing radioactive material, Brookhaven National Laboratory, Upton, NY; Report 90329-2009; 2008

The National Academies, Radiation source use and replacement, Committee on radiation source use and replacement, National Research Council, Washington, DC; 2008.

U.S. Nuclear Regulatory Commission, Issuance of order for increased controls for certain radioactive materials licensees, Washington, DC; NRC EA-05-090; 2005

Table 1. Radionuclides of Concern (USNRC 2005)

Radionuclide	**Quantity of Concern** (TBq)	**Quantity of Concern** (Ci)
Am-241	0.6	16
Am-241/Be	0.6	16
Cf-252	0.2	5.4
Cm-244	0.5	14
Co-60	0.3	8.1
Cs-137	1	27
Gd-153	10	270
Ir-192	0.8	22
Pm-147	400	11,000
Pu-238	0.6	16
Pu-239/Be	0.6	16
Ra-226	0.4	11
Se-75	2	54
Sr-90 (Y-90)	10	270
Tm-170	200	5,400
Yb-169	3	81