U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG-2166

Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material

Office of Federal and State Materials and
Environmental Management Programs

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: U.S. Nuclear Regulatory Commission
Office of Administration
Publications Branch
Washington, DC 20555-0001
E-mail: DISTRIBUTION.RESOURCE@NRC.GOV
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG-2166

Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material

Manuscript Completed: May 2014
Date Published: May 2014

Prepared by:
A. Gaudreau[1], P. Goldberg[1], S. Hawkins[1], J. Katanic[1],
W. Lee[1], G. Purdy[2], D. White[2], F. Pavlechko[3], A. True[3],
C. Gordon[4], R. Ragland[4], K. Lambert[5], and J. Thompson[6]

[1]Office of Federal and State Materials and
Environmental Management Programs
[2]Office of Nuclear Security and Incident Response
[3]Office of Chief Human Capital Officer Training and Development
[4]Region I
[5]Region III
[6]Region IV

Duane White, NRC Project Manager

Office of Federal and State Materials and
Environmental Management Programs

ABSTRACT

This document provides guidance to U.S. Nuclear Regulatory Commission (NRC) licensees or applicants on developing and implementing a physical protection program for the protection of risk-significant radioactive materials (e.g., category 1 and category 2 quantities of radioactive material). The intent of this information is to provide NRC licensees or applicants guidance with specific emphasis on physical security best practices. The approaches and methods in this document are not requirements; however, the NRC considers them to be acceptable for complying with the requirements in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material."

Paperwork Reduction Act Statement

This NUREG contains information collection requirements associated with 10 CFR Part 37 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These information collections were approved by the Office of Management and Budget (OMB), approval number 3150-0214.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

CONTENTS

APPENDICES

FIGURES

TABLES

ACKNOWLEDGMENTS

We dedicate this report to Adam Gaudreau who passed away on September 11, 2013, due to a car accident. Adam was a major contributor to this report and will be greatly missed.

We would also like to thank the individuals listed below for assisting in the development of this report. All participants provided valuable insights, observations, and recommendations.

U.S. Nuclear Regulatory Commission Staff

Gaudreau, Adam
Goldberg, Paul
Gordon, Craig
Hawkins, Sarenee
Katanic, Janine
Lambert, Kenneth
Lee, Willie
Pavlechko, Frank
Purdy, Gary
Ragland, Randolph
Thompson, James
True, Andrea
White, Duane

Organization of Agreement States

Mills, Grant (North Carolina Department of Health and Human Services)
Oesterle, Donald (California Department of Public Health)

U.S. Department of Energy's National Nuclear Security Administration Global Threat Reduction Initiative

Butler, Nicholas
Cuthbertson, Abigail
Haase, Michael
Hatcher, Kristina
Herdes, Gregory
Iliopulos, Ioanna

ABBREVIATIONS AND ACRONYMS

AC&D	alarm communication and display
Am-241	Americium-241
BMS	balanced or bias magnetic switch
CCTV	closed-circuit television
CFR	*Code of Federal Regulations*
Cf-252	Californium-252
Cm-244	Curium-244
Co-60	Cobalt-60
CPU	central processing unit
Cs-137	Cesium-137
CsCl	Cesium Chloride
DOE	U.S. Department of Energy
DHS	U.S. Department of Homeland Security
DSP	digital signal processor
DVD	digital video disk
DVR	digital video recorder
FBI	Federal Bureau of Investigation
FPS	frames per second
GPS	global positioning system
GTRI	Global Threat Reduction Initiative
HIPPA	Health Insurance Portability and Accountability Act
HVAC	Heating, Ventilation, and Air Conditioning
IAEA	International Atomic Energy Agency
IDD	in-device delay
IDS	intrusion detection system
IP	internet protocol
IR	infrared
Ir-192	Iridium-192
JPEG	Joint Photographic Experts Group
LLEA	local law enforcement agency
M&D	manufacturing and distribution
MPEG	Moving Picture Experts Group
NNSA	National Nuclear Security Administration
NRC	U.S. Nuclear Regulatory Commission
NVR	network video recorder
PIN	personal identification number
PIR	passive infrared
Po-210	Polonium-210
Pu-238	Plutonium-238
Pu-239	Plutonium-239
Ra-226	Radium-226

RDD	radiological dispersal device
RED	radiation exposure device
RMS	remote monitoring system
RSO	Radiation Safety Officer
Se-75	Selenium-75
Sr-90	Strotium-90
SUV	sports utility vehicle
Tm-170	Thulium-170
TVL	television lines
UL	Underwriters Laboratories, Inc.
UPS	uninterruptible power supply
U.S.	United States of America
VCR	video cassette recorder
VMD	video motion detection
Yb-169	Ytterbium-169

GLOSSARY OF TERMS

Access Control
A system for allowing only approved individuals to have unescorted access to the security zone and for ensuring that all other individuals are subject to escorted access.

Adversary
A person performing malevolent acts in pursuit of interests harmful to the facility; an adversary may be an insider or an outsider.

Aggregated
Accessible by the breach of a single physical barrier that would allow access to radioactive material in any form, including any devices that contain the radioactive material, when the total activity equals or exceeds a category 2 quantity of radioactive material.

Agreement State
Any State with which the U.S. Atomic Energy Commission or the U.S. Nuclear Regulatory Commission has entered into an effective agreement under Subsection 274b of the Atomic Energy Act of 1954, as amended.

Approved Individual
An individual whom the licensee has determined to be trustworthy and reliable for unescorted access in accordance with Subpart B, "Background Investigations and Access Control Program," of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material," and who has completed the training required by 10 CFR 37.43(c).

Background Investigation
The investigation conducted by a licensee or applicant to support the determination of trustworthiness and reliability.

Best Practice
A method or technique that has consistently shown results superior to those achieved with other means and that is used as a benchmark.

Category 1 Quantity of Radioactive Material
A quantity of radioactive material meeting or exceeding the category 1 threshold in Table 1 of Appendix A, "Category 1 and Category 2 Radioactive Materials," to 10 CFR Part 37.

Category 2 Quantity of Radioactive Material
A quantity of radioactive material that meets or exceeds the category 2 threshold but is less than the category 1 threshold in Table 1 of Appendix A to 10 CFR Part 37.

Diversion
The unauthorized movement of radioactive material to a location different from the material's authorized destination inside or outside of the site at which the material is used or stored.

Escorted Access
Accompaniment while in a security zone by an approved individual who maintains continuous direct visual surveillance at all times over an individual who is not approved for unescorted access.

False Alarm
An alarm that is generated without apparent cause.

Foreign Agent
A person who actively carries out the interests of a foreign country while he or she is located in another host country (e.g., United States)

Local Law Enforcement Agency
A public or private organization that has been approved by a Federal, State, or local government to carry firearms and make arrests and that is authorized and has the capability to provide an armed response in the jurisdiction where the licensed category 1 or category 2 quantity of radioactive material is used, stored, or transported.

Mobile Device
A piece of equipment containing licensed radioactive material that is either mounted on wheels or casters or is otherwise equipped for moving without a need for disassembly or dismounting, or it is designed to be hand-carried. Mobile devices do not include stationary equipment installed in a fixed location.

Movement Control Center
An operations center that is remote from transport activity and that maintains position information on the movement of radioactive material, receives reports of attempted attacks or thefts, provides a means for reporting these and other problems to appropriate agencies, and can request and coordinate appropriate aid.

Nuisance Alarm
The activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt.

Radiation Exposure Device
An object used to maliciously expose people, equipment, and/or the environment to ionizing radiation without dispersal of radioactive material.

Radiological Dispersal Device
The combination of radioactive material and the means (whether active or passive) to disperse that material with malicious intent without a nuclear explosion.

Risk-Significant Radioactive Material
For the purpose of this document, a category 1 or category 2 quantity of radioactive material as defined in Appendix A to 10 CFR Part 37.

Physical Protection Program
Integration of people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks.

Sabotage
Deliberate damage, with malevolent intent, to a category 1 or category 2 quantity of radioactive material, a device that contains a category 1 or category 2 quantity of radioactive material, or the components of the security system.

Safe Haven
A readily recognizable and readily accessible site at which security is present or from which, in the event of an emergency, the transport crew can notify and wait for the local law enforcement agency.

Security Zone
Any temporary or permanent area determined and established by the licensee for the physical protection of category 1 or category 2 quantities of radioactive material.

Target
The objective of an attack, which is also called the asset (e.g., category 1 or category 2 quantity of radioactive material).

Terrorists
A person or people who use violence to intimidate others, often for political purposes.

Trustworthiness and Reliability
Characteristics of an individual considered dependable in judgment, character, and performance such that unescorted access to category 1 or category 2 quantities of radioactive material by that individual does not constitute an unreasonable risk to the public health and safety or security. (A determination of trustworthiness and reliability for this purpose is based on the results from a background investigation.)

Unescorted Access
Solitary access to an aggregated category 1 or category 2 quantity of radioactive material or the devices that contain the material.

Violent Activists
A violent person or people who take part in criminal activities that are intended to achieve political or social change.

1. PURPOSE OF THE REPORT

The terrorist attacks of September 11, 2001, heightened the Nation's concerns regarding the use of risk-significant radioactive materials in a malevolent act. Such an attack has been of particular concern because of the widespread use of radioactive materials in the United States and abroad for industrial, medical, and academic purposes. Loss or theft of such materials, in risk-significant quantities, could lead to their diversion for malicious use in a radiological dispersal device (RDD) or a radiological exposure device (RED). An RDD is a device or mechanism that is intended to spread radioactive material from the detonation of conventional explosives or through other means. RDDs are considered weapons of mass disruption; few deaths would occur due to the radioactive nature of the event; however, significant social and economic impacts could result from public panic, decontamination costs, and the denial of access to infrastructure and property for extended periods of time. An RED is a device whose purpose is to expose people to radiation instead of dispersing radioactive material into the air like an RDD would.

In an effort to increase protection of risk-significant radioactive material, the U.S. Nuclear Regulatory Commission (NRC) recently finalized a new regulation in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material." This new rule provides the NRC's requirements for the physical protection program for any licensee that possesses an aggregated category 1 or category 2 quantity of radioactive material. The regulations at 10 CFR Part 37 can be accessed on the NRC Web site at http://www.nrc.gov/reading-rm/doc-collections/cfr/part037/. Appendix A, "Category 1 and Category 2 Radioactive Materials," to 10 CFR Part 37 provides the radionuclides and threshold values for category 1 and category 2 quantities of radioactive material, sometimes referred to as risk-significant radioactive materials.

This best practices document provides guidance to a licensee or applicant regarding some best practices that should be used for the development and implementation of a physical protection program. A best practice is a method or technique that has consistently shown results superior to those achieved by other means and that is used as a benchmark for completing a task. Note that a key strategic talent required when applying best practices to organizations is the ability to balance the unique qualities of an organization with the practices that it has in common with others.

This document also supplements the guidance provided to applicants and licensees in NUREG-2155, "Implementation Guidance for 10 CFR Part 37, 'Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material.'" NUREG-2155 can be accessed on the NRC Web site at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr2155/. The guidance in NUREG-2155 is in the form of questions and answers for each section or subsection of the regulation and provides explanations of the text in the rule.

The NRC recognizes that some licensee personnel with responsibilities related to the implementation of the requirements in 10 CFR Part 37 lack expertise in physical security and the development of physical protection programs, which may result in inconsistent application of security measures and in the potential vulnerability of licensed materials. The information in this document is intended to provide practical guidance to applicants and licensees with specific emphasis on security best practices and effective application of security technology (e.g., access authorization, intrusion detection, alarms, and cameras) that licensees may consider in developing or enhancing their security programs. The approaches and methods described in this document

are not requirements; however, the NRC considers them to be sound technical and procedural approaches to establishing effective security programs that will meet the requirements in 10 CFR Part 37.

2. AN EFFECTIVE PHYSICAL PROTECTION PROGRAM

An effective physical protection program integrates people, procedures, and physical security technology to protect the facility and assets (e.g., category 1 or category 2 quantities of radioactive material) from theft, diversion, sabotage, or other malevolent attacks. An effective physical protection program should also have good administrative measures, such as having an employee review process for determining who should have access to the security zone (e.g., trustworthiness and reliability determination), and a process for protecting the security-related information (e.g., security plan). Access authorization, access control, detection, delay, assessment, and response are some key elements for an effective physical protection program. Protection in depth for these elements is a critical component to the overall effectiveness of the physical protection program. A protection-in-depth strategy deters an adversary by requiring him or her to avoid or defeat a number of different protective measures (e.g., barriers and intrusion sensors) in sequence to access risk-significant quantities of radioactive material. In addition, this strategy deters the adversary by adding uncertainty, requiring different techniques and tools, and creating additional steps. The layered protection concept adds to a system's overall reliability by removing dependency on one barrier or system, which protects against a single point failure.

2.1 Determining the Objectives of the Physical Protection Program

The first step in developing a physical protection program is to determine the objectives of the program by (1) properly characterizing the facility operations and conditions, (2) identifying the target(s) (e.g., category 1 or category 2 quantities of radioactive material), and (3) defining the threat. Licensees are also encouraged to talk to stakeholders (e.g., other licensees, organizations, or businesses) with knowledge, experience, and expertise in developing a physical protection program. In addition, licensees should coordinate, to the extent practical, with the responding local law enforcement agency (LLEA) to achieve a comprehensive understanding of the facility and its response needs.

2.1.1 Characterizing the Facility

Before any decisions can be made concerning the level of protection needed, an understanding of what the facility is protecting is necessary. Because this important step is often missed, security systems are designed in a way that either overprotects a nonessential component or fails to adequately protect a vital portion of the facility. Therefore, a facility must be understood fully in terms of its limitations or constraints (e.g., space issues and power failure problems) and the requirements for its operations. If an organization views the physical protection program only as a required function that adds minimal value, establishing an integrated physical protection program will be hard. Therefore, the management of the organization must provide the requisite authority, leadership, support, and resources to the physical protection program.

The physical aspects of the facility are often the easiest area to characterize because this information can generally be found in blueprints and drawings of the facility. The physical characteristics of the facility should include the number and locations of rooms or buildings within the facility or complex and should identify the site boundary, number and location of access points (e.g., personnel doors, rollup doors, windows, and roof access points), existing physical security features (e.g., intrusion sensors and alarms, locks, chains, and barriers), and all infrastructure details (e.g., heat and air conditioning systems, ventilation ducts, communication systems, building construction materials, and power distribution systems). Other physical aspects of the facility that the organization should review when characterizing it

include an understanding of the surrounding area, such as the type of area (e.g., urban, suburban, and rural areas), neighborhood crime statistics, nearby businesses or facilities, topography, vegetation, wildlife, background noise (e.g., nearby airports, train yards, major highways, or electromagnetic interference), and climate and weather conditions. This information can be used to determine potential adversary paths into a facility, to identify the best areas to store risk-significant radioactive material, and to identify potential sources that may cause false or nuisance alarms.

Another major area that an organization needs to review and to fully understand when characterizing the facility is its operations. For example, is the facility involved in production, manufacturing, research, medical care, and academic activities? In addition, understanding the operating conditions, such as the working hours, off hours, emergency operations, and the types and number of personnel, is important. Reviewing the facility's operating procedures and conducting interviews with personnel (e.g., facility management and staff) should provide this type of information. Note that, although organizations may have well documented procedures, discovering that personnel use other undocumented procedures to do their work is not uncommon; therefore, for this reason, interviewing facility personnel is important. The physical protection program design must not cause an overly restrictive effect on the operations of the facility.

Another important aspect that an organization should consider when characterizing the facility is the regulatory requirements for operating the facility. Many authorities, such as the fire department and Federal, State, and local government agencies, may regulate the different operations within the facility. Not fully understanding these regulatory requirements or local ordinances when designing the physical protection program could cause major regulatory compliance issues.

When characterizing the facility operations, the designer of the physical protection program should also be aware of the facility's operations and should consider the safety aspects of those operations. The designer should take a balanced approach that weighs the safety and security needs of the facility. If the physical protection program design does not consider the safety needs, the organization can experience problems, such as possible injury to personnel, damage to equipment, regulatory compliance issues, and vulnerabilities in the physical protection program. For example, from a security perspective, the facility should have limited entry and exit points to minimize the possibility of unauthorized access by an adversary. However, from a safety standpoint, having open access may be very advantageous to allow a faster and safer exit point for personnel and entry of emergency responders in the event of an emergency (e.g., fire) or to allow an easier and safer method for installing, repairing, or replacing equipment. Another conflict between security and safety that could occur is if a fire starts in a room with limited access/exit points and activates the automatic sprinklers. In that instance, the water from the sprinklers could short out the electric door locks and possibly prevent the immediate exit of the personnel in the room or access for the emergency responders, or both.

2.1.2 Identifying the Target

Target identification provides the basis for designing the physical protection program. Identifying the target or targets enables an evaluation of what needs to be protected without considering the threat or level of difficulty to provide adequate physical protection. For the purposes of this document, the target would be category 1 or category 2 quantities of radioactive material or devices, or both, that contain such material as defined in Appendix A, "Category 1 and Category 2 Radioactive Materials," to Title 10 of the *Code of Federal Regulations* (10 CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material."

If a licensee does not have any single source that equals or exceeds the category 2 value in Appendix A to 10 CFR Part 37, it needs to examine its radioactive material inventory to determine whether it has multiple sources that individually do not equal or exceed the category 2 value; however, collectively, its activity adds up to an aggregated category 1 or category 2 quantity of radioactive material. The U.S. Nuclear Regulatory Commission (NRC) defines "aggregated" as accessible by the breach of a single physical barrier that would allow access to the radioactive material in any form, including any devices that contain radioactive material, when the total activity equals or exceeds a category 2 quantity of material.[1] To determine whether an aggregated category 1 or category 2 quantity of radioactive material exists, the licensee should use the guidance and sum of fractions calculation (unity rule) provided in Appendix A, "Category 1 and Category 2 Radioactive Materials," to NUREG-2155, "Implementation Guidance for 10 CFR Part 37, 'Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material,'" issued February 2013.

2.1.3 Defining the Threat

Defining the threat should be the next step in determining the objectives for the physical protection program. The definition of a threat should describe the potential types of adversaries. Generally, the types of adversaries are categorized into three broad groups: (1) outsiders, (2) insiders, and (3) outsiders working in collusion with insiders. Outsiders could include terrorists, criminals, violent activists, or foreign agents. Generally outsiders and insiders are driven by some type of motivation, which could include political or philosophical motivation (e.g., antinuclear or hate groups), economic motivation (e.g., financial gain), or a personal motivation (e.g., hatred toward a person or organization). Any employee within the company can pose as a potential insider threat, even managers and security personnel. Protecting against such insiders is a bigger challenge because they generally have some knowledge of the facility's operations or security systems, or both, and because they may have unescorted access to the facility or access to category 1 or category 2 quantities of radioactive material, or both. Insiders could serve several purposes that licensees should consider when defining the threat, such as passively providing information to an outsider; actively assisting in providing entry or exit from a secured area, disabling alarms or communications, or participating in a violent attack on the facility.

Licensees should consider different approaches when protecting against an outsider, insider, or outsider in collusion with an insider. Effective physical protection measures can deter or deny an outsider access to category 1 or category 2 quantities of radioactive material. In addition to effective physical protection measures, administrative security measures, such as having policies and procedures for authorizing access to material and information, ensuring proper handling of sensitive information, and verifying the trustworthiness and reliability of individuals can help deter and identify insiders. For outsiders in collusion with insiders, control of the critical assets (e.g., limiting the number of people with unescorted access and separate security controls for access to category 1 or category 2 quantities of radioactive material than for general facility access) should be added to the physical protection and administrative security measures.

Adversaries will use any tactic to increase their chances of achieving their objective. The primary tactics an adversary will use include force, stealth, and deceit. Force is when the adversary

[1] See Appendix A, "Category 1 and Category 2 Radioactive Materials," to 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material," for the threshold values for category 2 quantities of radioactive material.

overpowers the physical protection program without attempting to hide his or her intention. A stealth tactic is used when the adversary tries to enter and exit the facility secretly to achieve their goal. Deceit by an adversary involves the use of real or forged credentials to gain authorized access. Different groups of adversaries will use different tactics. For example, an insider adversary would benefit the most by using deceit to achieve his or her objective. An outsider, such as a terrorist, may use a combination of stealth and then force to achieve their objective. Consideration of the adversary tactic or combination of tactics should be part of the threat definition for the facility.

The licensee can generally obtain information regarding outsider threats, such as local criminals and extremist groups, from the LLEA. The NRC has processes in place to notify licensees and Agreement States of specific threat information that could affect licensees (e.g., issuance of a security advisory or an order recommending or requiring an increase in licensee security of risk-significant radioactive material). In addition, security managers within a facility should be made aware of any work force and labor issues/disputes within the facility because this information could be beneficial in identifying potential insider threats.

2.2 Key Elements of a Physical Protection Program

An effective physical protection program should properly incorporate the elements of access authorization (e.g., trustworthiness and reliability determination), access control (e.g., electronic card readers), detection (e.g., infrared motion sensors), delay (e.g., reinforced concrete walls), assessment (e.g., direct observation by approved individuals), and response (e.g., LLEA) to increase the likelihood that these elements will be able to deter, delay, detect, and provide enough time for the response force (e.g., LLEA) to arrive and stop the adversary from achieving his or her final objective (e.g., theft or diversion of category 1 or category 2 quantities of radioactive material). Some key points regarding these elements that the licensee should consider when developing a physical protection program are provided below. Later chapters of this document provide additional information regarding the implementation of these key elements.

2.2.1 Access Authorization

For the purposes of this document, access authorization refers to the administrative process that is used to determine who should be authorized unescorted access to risk-significant radioactive material or sensitive information, or both. Unescorted access in the security zone should only be granted to individuals who have been determined to be trustworthy and reliable and have an operational need for access. The access authorization process should ensure that the decision to grant access is based on an objective analysis of job functions and operational needs rather than on convenience or other subjective considerations. Limiting unescorted access to as few individuals as possible (i.e., those individuals whose trustworthiness has been verified) plays a key role in reducing the potential risk posed by insiders.

If possible, the access authorization function should be managed or performed, or both, by different parts of the organization. For example, the organization's human resources department or individual could perform the trustworthiness and reliability determination, the Radiation Safety Officer could determine who should be granted unescorted access to the risk-significant radioactive material and sensitive information, and the organization's security manager would control physical access (e.g., issue keys or keycards). This separation of functions provides checks and balances and audit points in the management system, and it ensures that no single person or part of the organization has authorization over the entire process for controlling access to the risk-significant radioactive material or sensitive information, or both.

2.2.2 Access Control

Access control is an important part in securing risk-significant radioactive material and sensitive information and should involve the use of the appropriate physical access controls and adherence to administrative processes (e.g., the organization's security policies and procedures). The physical access controls should control the movement of people or material into or out of the secured area (e.g., security zone) and should detect the actual or attempted access of unauthorized personnel. The physical access controls includes doors, walls, fences, locks, and electronic access control systems. The administrative process for access control should include the following key aspects:

- Issuance, control, and accounting of access media and codes (e.g., keys, identification cards, lock combinations, personal identification numbers, and alarm system codes)
- Requirements for access rights to controlled areas
- Termination of access rights when access is no longer needed
- Visitor management and escort procedures
- A change in keys, combinations, alarm system codes/passwords, and other access media when they are lost or compromised
- Operation and management of electronic access control systems (if applicable)

Licensees should also be alert for covert actions in preparation for an attempted theft, sabotage, or diversion. For example, such covert actions could include the theft and copying of keys to locked rooms or storage containers or the gaining of access to security codes for copying such codes onto duplicate key cards or for turning off the alarm system. Therefore, licensees should monitor, assess, and respond to actual or attempted unauthorized access to keys, security cards, codes (e.g., access and alarm codes), or other means that could be used in an attempt to gain unauthorized access to the risk-significant radioactive material in a security zone.

2.2.3 Detection

Detection is the first key function used to intercept an adversary from accomplishing a malevolent act. The earlier an adversary is detected, the greater the chances that the response force will be successful in intercepting the malevolent act. The detection system of an effective physical protection program should include the following attributes:

- The system has redundant critical elements (e.g., use of a balanced magnetic door sensor and an infrared motion sensor for the same room).
- The system has complementary technologies so that the adversary has to use a variety of defeat methods (e.g., use a passive infrared motion sensor and an active microwave motion sensor to detect the same area).
- The system has low nuisance and false alarm rates and has a high probability of detection.
- The system can detect tampering (e.g., loss or interruption in the alarm signal line).

- The system is reliable and robust for the type of operating environment (e.g., an outside or inside environment or an arctic or hot climate).

- The system is combined with a good assessment system. (Note that the detection function is not completed without assessing what was detected.)

- The system is regularly maintained and tested through a performance testing program. (See Section 3.6 of this report for more information).

2.2.4 Delay

After detection, delay is the next key function used to hinder an adversary from accomplishing a malevolent act. The purpose for delay is to slow down the adversary's progress so that the response force has the time to intercept the adversary before he or she can perform a malevolent act. Delay can be accomplished by using people (e.g., security force), barriers (e.g., reinforced concrete walls), and locks (e.g., high security door locks). The licensee should think through and plan, in detail, the delay system to ensure that it has addressed or considered every pathway to the target. When possible, the licensee should integrate the delay features into the facility design to help minimize the effects that it may have on the operation and safety of the facility. An effective delay system should consist of multiple types of delay mechanisms that would require an adversary to be well equipped with a variety of tools to defeat each barrier. The delay system should also be able to detect an adversary when he or she approaches a delay mechanism to identify his or her location/progress. Note that a delay mechanism without a detection capability associated with it is merely a deterrence (i.e., it may possibly discourage but not deter an adversary from going forward). The location of the adversary would not be known without detection, thus giving the adversary the time he or she needs to defeat the delay mechanism and to move to the next objective without detection.

2.2.5 Assessment

Assessment is an essential part of the detection function because it identifies the cause for an alarm (e.g., intruder or false alarm) and because it initiates the appropriate response. Assessment can be accomplished through physical checks from personnel or through the monitoring of video images from cameras (e.g., closed-circuit television). Personnel who perform assessments must be properly trained to interpret the authenticity of an alarm occurrence and must be capable of initiating a response. In addition, any personnel who may be responsible for performing an assessment should be deemed trustworthy and reliable. Personnel who perform physical assessments may be first to encounter an intruder; therefore, they must understand what to do in the event of an intrusion (e.g., whom to summon for help and how to summon help and when to take action and what type of protection measures should be taken).

The use of video assessment is considered a best practice for assessing an alarm. Using a video assessment system allows alarms to be rapidly assessed at a remote location without unnecessarily sending personnel into a potentially hazardous situation. The licensee should consider other key factors for using video assessment to assess alarms, as follows:

- The cameras should be available 24 hours a day and should be monitored at all times when the target (e.g., risk-significant radioactive material) is not under direct observation.

- The cameras, monitoring equipment, and personnel used to assess the alarms should be protected or located, or both, in a secure location that is not vulnerable to intruders.

- Assessment personnel should have a reliable and redundant means to summon help immediately (e.g., duress buttons and radios).

- Assessment video should be recorded for investigative purposes in case the adversary is successful in accomplishing the malevolent act or is not captured, or both.

Note that, after a period of time (e.g., a half an hour to an hour), human effectiveness at detecting suspicious events drops significantly when personnel view security television monitors. Therefore, the physical protection program should incorporate some detection sensor technology to assist in the detection function and to assist personnel who are remotely monitoring the detection areas.

2.2.6 Response

Response is the last key function that is used to stop an adversary from accomplishing a malevolent act. For the purposes of this document, the NRC expects that the LLEA would serve as the response force for the facility/site if an intrusion occurs by an adversary. The regulations at 10 CFR 37.5, "Definitions," define an LLEA as a public or private organization that has been approved by a Federal, State, or local government to carry firearms and to make arrests and that is authorized and has the capability to provide an armed response in the jurisdiction in which the licensed category 1 or category 2 quantity of radioactive material is used, stored, or transported. In addition, under 10 CFR 37.49(d), the NRC requires the licensee to request, without delay, an armed response from the LLEA for any unauthorized access involving an actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material.

The licensee should develop a response plan as part of the written security plan; such a plan should define the responsibility of the onsite or offsite response forces, or both. (See Appendix A to this report for more information on security plans.) The response plan should also include a plan for recovering the risk-significant radioactive material if the adversary is successful in taking the device or radioactive material. For effective response, the following actions should be taken:

- Provide the LLEA with sufficient detailed information about the facility or site and provide a description of the risk-significant radioactive material and the potential hazards associated with it.

- Provide the LLEA with updates of information about the facility, the risk-significant radioactive material, or the storage and use of the material changes.

- Ensure that reliable and redundant communications are always available (e.g., two-way radios and landline telephones).

- Conduct response training and exercises periodically to validate and improve response force readiness.

- Conduct periodic face to face meetings with the LLEA.

- Perform periodic testing of the alarm response with the LLEA.

3. ADMINISTRATIVE SECURITY MEASURES

Administrative security measures serve a key role in the development and implementation of the physical protection program. They are generally provided in the form of security policies or procedures, or both. Administrative security measures primarily provide information on how to manage and implement the physical protection program, and they should also focus on mitigating the insider threat. The administrative security measures should include the following key subject areas:

- Authorization requirements for access to risk-significant radioactive material and sensitive information
- A determination of the trustworthiness and reliability of individuals who require unescorted access to risk-significant radioactive materials (i.e., category 1 and category 2 quantities of radioactive material)
- Security training requirements for individuals responsible for security
- Procedures for protecting the risk-significant radioactive materials and sensitive information (e.g., security plan)
- Maintenance and testing of security equipment (e.g., detection sensors, alarms, and video assessment equipment)
- Compensatory security measures that address security equipment failures or emergencies, or both, without degrading the physical protection program
- Response planning and coordination

3.1 Access Authorization Program

Access authorization is the administrative process for determining who should be approved for unescorted access to risk-significant radioactive material or sensitive information, or both. The main objective of the access authorization program is to ensure that individuals who have unescorted access to category 1 or category 2 quantities of radioactive material are trustworthy and reliable and do not constitute an unreasonable risk to the public health and safety or security of the radioactive material. The U.S. Nuclear Regulatory Commission (NRC) requires licensees that possess an aggregated quantity of radioactive material at or above the category 2 threshold, as defined in Appendix A, "Category 1 and Category 2 Radioactive Materials," to Title 10 of the *Code of Federal Regulations* (10 CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material," to establish, implement, and maintain their access authorization program in accordance with 10 CFR 37.21, "Personnel Access Authorization Requirements for Category 1 or Category 2 Quantities of Radioactive Material." Unescorted access shall only be granted to those individuals with job duties that require unescorted access to category 1 or category 2 quantities of radioactive material (10 CFR 37.21(c)(3)). Therefore, the decision to grant unescorted access should be based on objective analysis of job functions and operational need rather than on convenience or other subjective considerations. Limiting unescorted access to as few individuals as possible also plays a key role in reducing the potential risk posed by insiders.

Representatives from different departments within the organization, such as human resources, the radiation safety office, facility management, and security, should develop criteria jointly for determining which job function or individual, or both, needs to have unescorted access. Generally, only the minimum number of job functions that specifically require access should be recommended for unescorted access authorization. Some examples of job functions that may require access include regular users of the radioactive material or device containing the material (e.g., authorized users of the material, such as researchers, doctors, and radiographers), the Radiation Safety Officer (RSO), and radiation safety personnel. Some job functions may not require regular access but should be granted unescorted access because of their role in controlling access or emergency response (e.g., security personnel and specific safety management personnel). Other job functions may require access but would not warrant unescorted access because of the infrequent need for access or the specific nature of the position. In these cases, access could be allowed under the escort of an approved individual. For example, such positions can include janitorial workers, facility management workers, and visiting scientists or students. After deciding which job function or individual, or both, needs to have unescorted access to risk-significant radioactive material or sensitive information, or both, the licensee must perform a background investigation on the individual (10 CFR 37.25(a)). The background investigation is a tool to obtain information necessary to determine whether an individual is trustworthy and reliable and should be permitted unescorted access.

3.1.1 Background Investigation

Background investigations must cover at least the 7 years preceding the date of the investigation or since the individual's 18th birthday, whichever is shorter. Consistent with 10 CFR 37.25(a), the background investigation must include at a minimum the following information:

- fingerprinting and a Federal Bureau of Investigation (FBI) identification and criminal history records check, as defined in 10 CFR 37.27, "Requirements for Criminal History Records Checks of Individuals Granted Unescorted Access to Category 1 or Category 2 Quantities of Radioactive Material"
- verification of true identity
- employment history and education verification
- character and reputation determination

Fingerprinting an individual for an FBI criminal history records check is an important element of the background investigation. It can provide comprehensive information on an individual's recorded criminal activities within the United States and its territories and on the individual's known affiliations with violent gangs or terrorist organizations.

When verifying the true identity of an applicant for unescorted access authorization, the licensee should examine "official identification documents" to determine whether they reasonably appear to be genuine and whether they relate to the individual. The licensee may use identity documents issued by a State or local government or by the Federal Government as long as these documents contain a photograph and information, such as name, date of birth, gender, height, eye color, and address. These documents include passports, drivers' licenses, and identification cards issued by Government entities. The licensee may use one or more of the documentation types required by the U.S. Citizenship and Immigration Service's I-9 Form that applicants use to apply for eligibility for employment. The licensee should compare the documents (e.g., driver's license) to the information provided by the applicant.

The licensee can generally verify an individual's employment history and education by contacting previous employers and academic institutions. When contacting the previous employers, the licensee should ask specific questions regarding an individual's employment to verify that he or she is being honest about his or her work history. For verification of education, the licensee may also ask the individual to provide documentation that verifies his or her education (e.g., a high school diploma or college transcripts, or both).

The licensee should complete reference checks to determine the character and reputation of the individual who has applied for unescorted access authorization. Unless other references are unavailable, the licensee should not conduct a reference check with any person who is known to be a close member of the individual's family, including, but not limited to, the individual's spouse, parents, siblings, or children, or with any individual who resides in the individual's permanent household (10 CFR 37.25(a)(5)). In addition, the licensee should limit the reference check to whether the individual has been, and continues to be, trustworthy and reliable. The licensee should corroborate derogatory information obtained during reference checks, to the extent possible, before considering the information to be disqualifying. The following questions provide examples that the licensee should consider asking when conducting the reference check:

- Would you trust the individual with high value assets?
- Would you consider the individual to be trustworthy and reliable?
- Have you ever witnessed anything in the individual's behavior that would cause you to question his or her trustworthiness or reliability, or both?

A licensee may also take into account a number of different kinds of information from a number of sources to make a determination about an individual's character and reputation as long as the information is clearly pertinent to his or her likely conduct or behavior if he or she were granted unescorted access. In addition to records of any arrest or conviction (e.g., local or Federal) as an adult or juvenile, other information that could be used includes, but is not limited to, the following:

- evidence of false or deceitful statements
- loss of a driver's license
- repeated high-speed traffic or other violations that indicate a reckless disregard for the safety or security of others
- poor credit history[1]
- a recent bankruptcy, foreclosure, repossession, or garnishment of income
- repeated nonpayment of alimony, child support, or lawfully incurred financial obligations for periods of months
- repeated instances of personal harassment

[1] The licensee should check to see whether State laws or local ordinances prohibit employment discrimination based on credit history.

- conduct or behavior that would violate any of the licensee's corporate or professional code of ethics or workplace conduct

Consistent with 10 CFR 37.23(c), before it can initiate a background investigation, the licensee must inform the individual being investigated of such action, and the individual must sign a consent form authorizing the licensee to conduct the background investigation. The licensee must first explain to the individual that a background investigation is being conducted and then explain the potential consequences if the individual does not agree to the background investigation. (For example, he or she may not have unescorted access to risk-significant radioactive material.) The signed consent shows that the individual has been provided the appropriate explanation and indicates his or her understanding that a background investigation will be conducted. The signed consent must also indicate that authorization has been given to share personal information with other individuals or organizations, as necessary, to complete the background investigation. Annex B, "Sample Consent Form for Background Investigations," of NUREG-2155, "Implementation Guidance for 10 CFR Part 37, 'Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material,'" issued February 2013, provides a template for a possible consent form that a licensee can adapt for its use.

Note that the NRC requires licensees to establish and maintain a filing system and written procedures to protect individuals from unauthorized disclosure of records and personal information produced from background investigations under 10 CFR Part 37 (10 CFR 37.31(a)). The collected background information will likely contain personally identifiable information and should only be provided to authorized individuals. Under Section 149(c)(2)(D) of the Atomic Energy Act of 1954, as amended, the Commission must prescribe requirements for the use of background investigation information "to protect individuals subject to fingerprinting under this section from misuse of the criminal history records." The licensee should, as a best practice, store background investigation documentation in a locked drawer or file cabinet.

3.1.2 Trustworthiness and Reliability Determination

The NRC defines trustworthiness and reliability as characteristics of an individual considered dependable in judgment, character, and performance such that unescorted access to category 1 or category 2 quantities of radioactive material by that individual does not constitute an unreasonable risk to the public health and safety or security. When a person's life history shows evidence of unreliability or untrustworthiness, a licensee may question whether that person can be relied on and trusted to exercise the responsibility necessary for having access to risk-significant radioactive materials.

When evaluating the relevance of an individual's conduct, the licensee should consider the following factors:

- nature, extent, and seriousness of the conduct
- circumstances surrounding the conduct, including evidence indicating whether it was deliberate
- frequency and timing of the conduct (e.g., did it take place recently)
- individual's age and maturity at the time of the conduct
- extent to which the individual's participation in the conduct was voluntary

- presence or absence of rehabilitation and other permanent behavioral changes
- motivation for the conduct
- potential for pressure, coercion, exploitation, or duress as a result of the conduct
- likelihood of continuation or recurrence of the conduct

Each case should be judged on its own merits, and, in every case, the trustworthiness and reliability determination should be based on an accumulation of information that supports a positive finding before granting unescorted access. The licensee should consider the following items:

- whether the information collected is consistent and adequate
- whether the applicant's true identity can be reasonably verified by comparing applicant-provided identification and personal history data to pertinent information from the background investigation and other data sources
- whether inconsistencies identified by the licensee's review or investigation are intentional, innocent, or an oversight

Willful or intentional acts of omission or untruthfulness could be grounds for denial of unescorted access.

When a licensee submits fingerprints, it will receive an FBI identification and criminal history record documenting any criminal history since the individual's 18th birthday. The criminal history records check is used to evaluate whether the individual has a record of criminal activity that may compromise his or her trustworthiness and reliability. Identification of a criminal history through the FBI criminal history records check or a discretionary local criminal history check does not automatically indicate an individual's unreliability or untrustworthiness. The licensee will have to judge the nature and timing of the criminal activity. The licensee may authorize individuals with criminal records to have unescorted access to radioactive materials based on a documented evaluation of the basis for determining that the employee or applicant is reliable and trustworthy, notwithstanding his or her criminal history. When evaluating the results of the criminal history records check, the licensee should consider, at a minimum, whether the subject individual did the following:

- Committed, attempted to commit, aided, or abetted another individual who committed or attempted to commit any act of sabotage, espionage, treason, sedition, or terrorism.
- Publicly or privately advocated actions that may be harmful to the interest of the United States, or publicly or privately advocated the use of force or violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means.
- Knowingly established or continued a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, or revolutionary; with an espionage agent or other secret agent or representative of a foreign nation whose interests may be inimical to the interests of the United States; or with any person who advocates the use of force or violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means. (Ordinarily, the licensee

should not consider chance or casual meetings or contacts limited to normal business or official relations.)

- Knowingly joined or engaged in any activity in sympathy with, or in support of, any foreign or domestic organization, association, movement, group, or combination of persons who advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or any State or any subdivisions thereof by unlawful means or who advocate the use of force and violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means. (Ordinarily, the licensee should not consider chance or casual meetings or contacts limited to normal business or official relations.)

- Deliberately misrepresented, falsified, or omitted relevant and material facts from documentation provided to the licensee.

- Had been convicted of a crime(s) that indicates poor judgment, unreliability, or untrustworthiness.

In addition, licensees may consider how recently such indicators occurred and other extenuating or mitigating factors in their determinations. Section 149c(2)(B) of the Atomic Energy Act of 1954, as amended, requires that the information obtained as a result of fingerprinting be used solely for the purposes of making a determination as to a person's suitability for unescorted access. Such a determination is not a hiring decision, and the NRC does not intend for licensees to use this guidance for such purposes. In addition, licensees should not make a final determination based solely on criminal history check information involving an arrest of more than 1 year old for which no information is available on the disposition of the case or an arrest that resulted in dismissal or acquittal of the charge. In addition, a determination that a particular individual is unsuitable for unescorted access does not necessarily mean that he or she is unsuitable for escorted access or for some other position that does not involve NRC-regulated activities.

The licensee should consider all information collected in making a trustworthiness and reliability determination for unescorted access. Licensees should substantiate and document potentially disqualifying information obtained from confidential or unnamed sources and should not use this information as the sole basis to deny access authorization unless it is corroborated. Licensees should establish criteria that would disqualify someone from being granted authorized access. In every case, the licensee should evaluate trustworthiness and reliability based on an accumulation of information that supports a finding with reasonable assurance. The trustworthiness and reliability determination is designed to identify past actions that give reasonable assurance of an individual's reliability.

In addition to the criminal history records check, licensees may want to consider whether the subject individual has exhibited the following behaviors:

- impaired performance attributable to psychological or other disorders

- conduct that warrants referral for criminal investigation or results in an arrest or conviction

- an indication of deceitful or delinquent behavior

- attempted or threatened destruction of property or life
- suicidal tendencies or an attempt at suicide
- illegal drug use or the abuse of legal drugs
- alcohol abuse disorders
- recurring financial irresponsibility
- irresponsibility in the performance of assigned duties
- inability to deal with stress or the appearance of being under unusual stress
- failure to comply with work directives
- hostility or aggression toward fellow workers or authority
- uncontrolled anger
- violation of safety or security procedures
- repeated absenteeism
- significant behavioral changes, moodiness, or depression

These indicators are not meant to be all-inclusive or intended to be disqualifying factors. Licensees may also consider extenuating or mitigating factors in their determinations.

Consistent with 10 CFR 37.23(g), the licensee must notify individuals denied authorization for unescorted access and must ensure that these individuals are informed of the grounds for its denial or termination of unescorted access authorization. In addition, the licensee must provide such individuals an opportunity upon request to review the denial or termination and additional relevant information. Before a final adverse determination is made, the licensee must also provide the individuals with an opportunity to correct any inaccurate or incomplete information that is found during the background investigation. Therefore, the licensee should, as a best practice, ensure that its procedures address its expectations for the performance and documentation of background investigations and trustworthiness and reliability determinations.

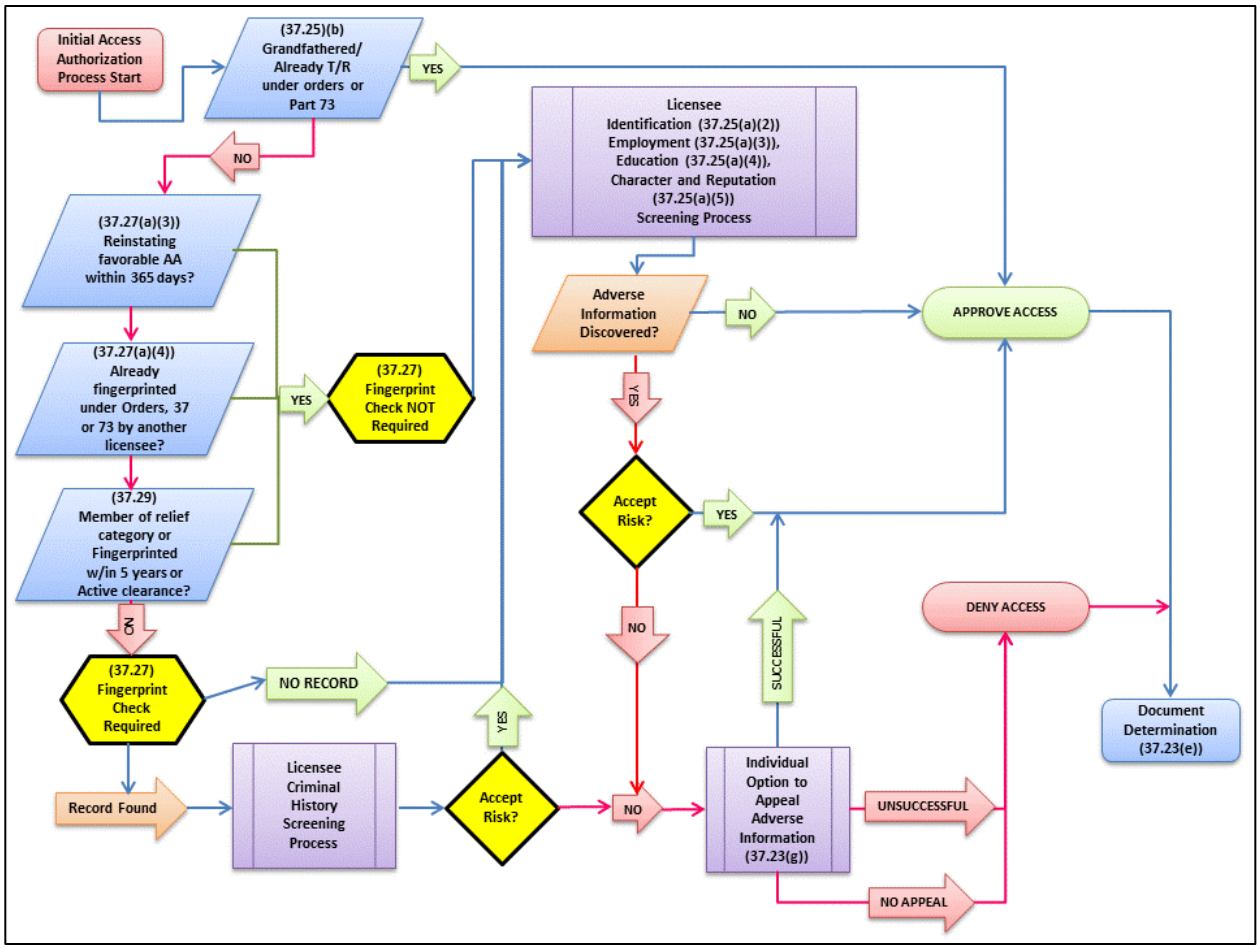

Figure 3-1 Access authorization process

3.1.3 Managing Access

In addition to establishing the process for who should be approved for unescorted access to the risk-significant radioactive materials or sensitive information, or both, establishing the policies and procedures for managing or controlling access is important. The licensee should also direct its policies and procedures for managing access with the objective of mitigating the insider threat and should ensure that they do the following:

- Issue, control, and account for access media (e.g., keys, identification cards, and combinations).
- Establish specific access rights for approved individuals (e.g., only allow access between certain hours, such as 9 a.m. to 5 p.m., or limit access to specific areas within the facility or security zone, or both).
- Terminate access rights when access is no longer authorized.
- Establish visitor management and escorting procedures.
- Change keys, combinations, and other access media when they are lost or compromised.

- Audit access media periodically to confirm that keys and cards are accounted for.
- Ensure the operation and management of electronic access control systems (if applicable).
- Periodically review unescorted access authorization determinations to ensure that they are still valid.

If possible, the functions of access authorization, trustworthiness and reliability determinations, and access media control should be separated to ensure no single entity controls all elements for providing unescorted access to the risk-significant radioactive material or sensitive information, or both. For example, the organization's human resources department or individual could perform the trustworthiness and reliability determination, the RSO could determine who should be authorized access to the risk-significant radioactive material, and the organization's security manager would control physical access (e.g., issue keys or keycards). This separation of functions also provides checks and balances and audit points in the access management system.

3.2 Physical Security Plan

For the purposes of this NUREG report, the security plan is a written document that describes the licensee's overall security strategy to ensure the integrated and effective functioning of the security program required by the NRC (Subpart C, "Physical Protection Requirements during Use," of 10 CFR Part 37). Consistent with 10 CFR 37.43, "General Security Program Requirements," the security plan must, at a minimum, describe the measures and strategies used to implement NRC requirements and must identify the security resources, equipment, and technology used to satisfy the requirements. As a best practice in explaining its overall strategy, the licensee should ensure that its security plan describes any site-specific conditions that affect how it will implement NRC requirements. An adequate plan requires a licensee to analyze the particular security needs of its individual facilities and to explain clearly how it will implement its chosen security measures to ensure that they work together to meet the applicable performance objectives.

To ensure the integrated and effective functioning of the security program and to facilitate its meeting the program review requirements in 10 CFR 37.33, "Access Authorization Program Review," the licensee should also consider describing a process in the security plan for identifying and implementing corrective actions or compensatory measures in the event of a failure of personnel or equipment to perform as specified or function as required. Note that the NRC requires that the individual with overall responsibility for the security program must review and approve the security plan (10 CFR 37.43(a)(2)). The licensee can designate this individual. The individual can be the company president, Director of Security, the RSO, or any other individual designated as the responsible person for the security of all the licensee's category 1 or category 2 quantities of radioactive material.

A licensee must revise its security plan, as needed, to ensure effective implementation (10 CFR 37.43(a)(3)). The individual with overall responsibility for the security program must review and approve any revision, and the licensee must instruct the affected individuals on the revised plan before it implements the changes (10 CFR 37.43(a)(3). Some of the following reasons may require the licensee to revise its security plan:

- a need to make changes to the physical protection program based on the results of the annual security program review

- a need to increase the quantity of radioactive material that it has aggregated at a given location

- a need to move the location of a storage area for an aggregated quantity of radioactive material

- a need to alter its facility in a way that could affect the security of the risk-significant radioactive material

- changes made to the measures that it relies upon to comply with 10 CFR Part 37

Appendix A of this NUREG report provides information that should be considered for developing a security plan.

3.3 Security Procedures

Consistent with 10 CFR 37.43(b)(1), the licensee must develop and maintain written procedures that document how the physical protection requirements and the security plan will be met. Generally, the security procedures should address how the licensee will implement the applicable features required by Subpart C of 10 CFR Part 37. Depending on the licensee and its operating requirements, these features would require its procedures to (1) address training, (2) establish and maintain security zones, and (3) establish the monitoring, detection, assessment, and response measures; maintenance and testing measures; and the reporting of events, and (4) periodically review the program. The written procedures should address how the licensee will respond to a range of foreseeable events common to the type of license. Examples of such events could range from an inadvertent unauthorized access that would not require a response from a local law enforcement agency (LLEA) response to a malevolent intrusion that would require LLEA intervention. These procedures should include, if applicable, provisions for immediate response, after-hour notification of LLEAs and the licensee's individual who is responsible for security, the handling of both radiation safety and security-related types of emergencies, and events at temporary jobsites.

Procedures should also address the roles of the licensee's staff and, where applicable, its contractors. The licensee's staff and contractors should have a clear understanding of their responsibilities and constraints in an emergency along with step-by-step instructions and clear guidelines for whom to contact. However, note that when developing these security procedures, the licensee should not compromise facility operational safety, occupational safety, fire safety, and emergency planning at the facility. In addition, the actual security procedures should be standalone documents, and an appendix to the security plan could include them.

3.4 Information Protection

The intent of information protection is to prevent unauthorized access to sensitive information. Sensitive information is considered any information whose unauthorized disclosure (or modification, alteration, destruction, or denial of use) could compromise the security of radioactive material and associated facilities or may otherwise assist in the carrying out of a malicious act against a facility, organization, or transport. Such information could include, for example, physical protection information about a facility (e.g., security plan, access codes,

and alarm system codes/passwords), the location and transport of risk-significant radioactive material, or details of the response capabilities to a specific type of threat.

The NRC requires that licensees authorized to possess category 1 or category 2 quantities of radioactive material must limit access to, and unauthorized disclosure of, their security plan, implementing procedures, and the list of individuals who have been approved for unescorted access (10 CFR 37.43(d)(1)). Efforts to limit access must include the development, implementation, and maintenance of written policies and procedures for controlling access to, and for the proper handling and protection against unauthorized disclosure of, the security plan and implementing procedures. In addition, licensees must evaluate an individual's need to know before allowing access to the security documents; if the individual has not been approved for unescorted access, he or she must undergo a background investigation to determine his or her trustworthiness or reliability before being provided the protected information (10 CFR 37.43(d)(3)).

The licensee's information protection policies and procedures should include the following items:

- a general performance requirement that each person who produces, receives, or acquires the licensee's sensitive information ensures that such information is protected against unauthorized disclosure
- instructions on how to protect sensitive information while it is in use, storage, and transit
- preparation, identification or marking, and transmission of documents or correspondence containing the licensee's security program information
- instructions on how access to the licensee's security program information must be controlled
- methods for the destruction of documents that contain security program information
- procedures for the use of automatic data-processing systems that contain security program information
- instructions for the removal of documents from the licensee's protected information category when they become obsolete or no longer sensitive

3.5 Security Training

All personnel within a facility that contains risk-significant radioactive material should have sufficient security training to enable them to understand the need for, and importance of, security at the facility and to recognize a security event and know what to do and whom to contact in such an event. This training helps to promote a strong security culture within the organization. Personnel with particular security responsibilities or functions require additional specific knowledge, skills, and abilities training, including the use of security equipment, to enable them to effectively perform these security functions.

The NRC does require the licensee to provide security training to its staff (10 CFR 37.43(c)). The training must cover the security program and its procedures for securing category 1 or category 2 radioactive materials, the purpose and function of the security measures, and the individual's responsibilities for reporting a security incident. The extent of the training should be

commensurate with the individual's potential involvement in the security of category 1 or category 2 quantities of radioactive material.

A licensee's training program should be evaluated to ensure that each individual with responsibility for any aspect of the security program has the requisite knowledge, skills, and abilities to carry out the responsibility effectively. Therefore, the minimum scope of a training program should identify these individuals and identify the working knowledge, skill sets, and capabilities they need to carry out their assigned duties and responsibilities for effective implementation of the licensee's security plan. The following examples are appropriate subjects for training:

- the controls that are in place to prevent unauthorized access to material
- the purpose and functional requirements of the licensee's alarm and access control systems
- notification procedures in the event of an unauthorized access for potential malevolent activities
- ways to confirm quickly and accurately whether an intrusion is likely to be intentional or accidental

In addition, an adequate program should train employees to identify any condition(s) that causes or may cause a violation of NRC requirements. In addition, it should train employees to identify and report any suspicious activity related to possible theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material. Suspicious activity could include unusual or suspicious behavior by employees or contractor employees with routine access to areas of the site or equipment related to the control of access to a security zone. An adequate program should also cover the operation of primary and backup communication systems for such reporting.

The licensee's staff members should have a clear understanding of their individual responsibilities and constraints in an emergency, and training should provide step-by-step instructions and clear guidelines on what they should do and whom they should contact in an emergency. In addition, the training should provide step-by-step instructions and clear guidelines on the proper performance of testing and maintenance activities. Training does not need to be in a classroom and can be performed as a part of on-the-job training. Training may be organized by subject area as well. For example, the licensee might train most of its employees on escort responsibilities and general alarm response. The licensee should train those employees who will be conducting surveillance on what to look for and how to respond to something that they that is unusual.

The licensee must also provide refresher training at least every 12 months and when significant changes have been made to the security program (i.e., 10 CFR 37.43(c)(3)). The refresher training should address the following items:

- any changes to the security program since the last training
- any changes in the assigned responsibilities of individual trainees that would require new training
- recent information on any relevant security issues or lessons learned

- relevant results from the program review or any NRC inspections

- relevant operating experience from the maintenance and testing program for security systems or system components

In addition, a licensee should consider providing refresher training after a security-related event so that affected or potentially affected employees can obtain a timely understanding of what happened and guidance on how to avoid or mitigate the consequences of a recurrence.

3.6 Maintenance and Testing Program

The maintenance and testing program should define the steps, procedures, and schedules for ensuring that all components of the security system are operating effectively or that they are returned to an operating capability as soon as possible. The program should specifically address both preventive and corrective actions and should be integrated as much as possible into the physical protection program while recognizing the sensitive nature of the security system.

The NRC requires the licensee to implement a maintenance and testing program to ensure that intrusion alarms, associated communication systems, and other physical components of the systems used to secure or detect unauthorized access to radioactive material are maintained in operable condition and that they are capable of performing their intended function when needed. The licensee should inspect and test the equipment that it relies on to meet security requirements for operability and performance at the manufacturer's suggested frequency. If manufacturer does not provide a suggested frequency, the licensee must perform the testing at least annually, but not to exceed 12 months (10 CFR 37.51(a)).

For the maintenance and testing program, the licensee, at a minimum, should do the following:

- Identify all alarms, communication systems, and other physical components necessary to secure radioactive materials or to detect unauthorized access to them.

- Specify the intended function of each component identified in the program and the minimum performance required to fulfill that function.

- Specify the test(s) that it will conduct on each component and identify the minimum quantitative or qualitative test results that are required for finding the component operable and capable of performing its intended function.

- Identify the testing equipment that it will use and prescribe any device-specific procedures necessary for the use or maintenance of this equipment.

- Identify the measures that it will apply to ensure that the testing equipment used in the program will perform in-service as expected.

- Prescribe procedures for the routine maintenance of each intrusion alarm, communications system, and physical component of both the system used to secure the subject radioactive material and the system used to detect unauthorized access.

- Require a written record for each test and maintenance activity performed on the security or detection system.

The licensee must maintain records on the maintenance and testing activities for 3 years (10 CFR 37.51(b)). For each maintenance activity, a record should identify the following items:

- name(s) of the person(s) who performed the maintenance
- date that the maintenance was performed
- component(s) or system(s) on which the maintenance was performed
- purpose of the maintenance, identifying, as appropriate, the deficiencies in operability or performance
- any maintenance activities needed to remove any deficiency in the operability or performance of the component or system

For each testing activity, a record should identify the following items:

- name(s) of the person(s) who performed the testing
- date of the testing
- component(s) or system(s) tested
- purpose of the testing
- performance expected to fulfill the intended function of the component or system
- results of the testing
- any maintenance activities needed to remove any deficiency in the operability or performance of the component or system

3.7 Contingency Planning

Contingency planning is an important part of ensuring the security and accountability of the risk-significant radioactive materials in the event of an emergency situation or an unexpected event that could affect the security of the risk-significant radioactive material. Contingency procedures should be developed that, at a minimum, take into account abnormal events that have an increased probability of occurring at the facility. The following examples are some of events that the licensee should consider:

- an unexpected evacuation (e.g., bomb threat or fire)
- serious natural events that have an increased probability of occurring in the area in which the facility or site is located (e.g., floods, earthquake, and tornado)
- damage or destruction of the facility or security zone, or both, which may require the need to move or recover the risk-significant radioactive material

- loss of all power, including backup power

- loss of all outside communications (e.g., radio, cell phone, and landline) or an inability to contact the response force

The licensee should develop contingency procedures with input from various components within the facility, such as company management; facility safety personnel; environmental or radiation safety personnel, or both; the LLEA; fire department; and other public safety agencies (i.e., NRC or Agreement State regulators). Those individuals who will have a role in the contingency procedures (e.g., security personnel and the RSO) must be properly trained on the contingency procedures. In addition, the contingency procedures must include plans for how to get the facility back to normal operations in a timely manner.

3.8 Response Planning and Coordination

The licensee must coordinate, to the extent practicable, with an LLEA (response force) for responding to threats to its facility, including any necessary armed response (i.e., 10 CFR 37.45, "LLEA Coordination"). The coordination activities could involve meetings, telephone conferences, plant tours, training in radiation safety, tabletop exercises, and other communications to provide information that would assist the LLEA in responding to an event when necessary. The licensee should develop a response plan as part of the written security plan that defines the responsibility among onsite or offsite LLEA or both. The response plan should also include a plan for recovering the risk-significant radioactive material if the adversary is successful in taking the material. The licensee must provide the LLEA with descriptions of its facilities, the risk-significant radioactive materials, and its security measures (10 CFR 37.45(a)(1)).

The licensee must also state that it will request a timely armed response by the LLEA to any actual or attempted theft, sabotage, or diversion of the risk-significant radioactive material (10 CFR 37.45(a)(2)).

A timely and effective response to a security incident is part of an effective physical protection program. Because certain situations may necessitate an armed response, the licensee should coordinate a strategy that is consistent in scope and timing with realistic potential vulnerabilities of the subject radioactive material well in advance with the LLEA. Such coordination would also provide the responsible LLEA with an understanding of the potential consequences associated with the malevolent use of the risk-significant radioactive material and would enable the LLEA to determine the appropriate priority of its response. The LLEA response would be necessary to interdict and disrupt an attempted theft, diversion, or sabotage of the radioactive material and to establish possible offsite coordination to protect public health and safety; recover stolen material; and mitigate the potential consequences of a theft, diversion, or sabotage of radioactive material.

Examples of information that a licensee could discuss with the LLEA include, but are not limited to, the following:

- types and quantities of devices and radioactive material possessed

- potential hazards associated with loss of control of the devices and radioactive material

- specific facility information (i.e., contact information, floor plans, entrances, points of egress, or other information)

- site-specific physical protection measures that the licensee employs to delay an adversary from gaining access to the radioactive material

- established protocol for contacting the LLEA in response to an event

- licensee and LLEA points of contact for plans to recover stolen radioactive material that has been removed from the facility

The licensee should also consider whether the LLEA could provide the needed armed response at all times, day or night, 7 days a week. Some LLEAs are on duty only during specified hours. In such cases, the licensee will have to identify, and coordinate with, the closest LLEA that can provide an armed response and arrest perpetrators when the primary LLEA is off duty. In addition, the licensee must document its coordination efforts, and it should include the dates, times, and locations of meetings and a list of licensee and LLEA staff members present at the meetings (10 CFR 37.45(c)).

4. PHYSICAL SECURITY BEST PRACTICES THAT APPLY TO ALL FACILITIES

This chapter provides the protective measures and best practices that a licensee should use when designing and implementing a physical protection program. This chapter primarily focuses on physically protecting the security zone; however, the licensee should consider the protection measures described below for use throughout the facility. The U.S. Nuclear Regulatory Commission (NRC) defines the security zone as the area (temporary or permanent) determined and established by the licensee for the physical protection of category 1 or category 2 quantities of radioactive material. Using a protection-in-depth strategy and a balanced approach when designing and implementing the program is the key to establishing an effective physical protection program.

A protection-in-depth strategy means that an adversary must avoid or defeat a number of protective measures in sequence to accomplish his or her goal. For example, an adversary might need to bypass or defeat two intrusion sensors and two barriers before gaining access to the security zone. The actions and amount of time necessary to bypass or defeat each measure may not be equal and the effectiveness of each measure may be different; however, each measure requires a distinct act while the adversary is moving along the path. The following goals are necessary to design a protection-in-depth strategy for the physical protection program:

- Increase the adversary's uncertainty about the physical protection program.
- Require the adversary to more extensively prepare before he or she attacks the facility.
- Create additional steps that may cause the adversary to fail or abort the mission.

In addition, when designing the physical protection program, the licensee should consider how all the different protective measures (e.g., an intrusion detection system and video assessment system) will work together. Integration of the protection program requires a balance among the security hardware, personnel, and operational procedures.

Note that Appendices B–H provide specific best practices that different types of licensees (e.g., self-shielded irradiator, well logging, radiography, and medical) should consider. The information in these appendices is meant to highlight the specific best practices, which are described in more detail in this chapter and Chapter 5. In addition, Appendix I to this document provides information on the Global Threat Reduction Initiative (GTRI), which is a voluntary program that licensees can participate in and which is sponsored by the U.S. Department of Energy's National Nuclear Security Administration (NNSA). Under this program, GTRI security experts provide security assessments, share observations, and make recommendations for enhancing the physical security of risk-significant radioactive material. Note that the GTRI security enhancements would be supplementary to, and consistent with, NRC and Agreement States security requirements. However, the GTRI voluntary program does not replace or diminish the licensee's responsibility to comply with the requirements in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material," or other NRC regulatory requirements.

4.1 Defining the Security Zone

The regulations at 10 CFR 37.47, "Security Zones," the licensee to use and store all aggregated category 1 and category 2 quantities of radioactive material within its established security zones. Permanent or temporary security zones must, at a minimum, allow unescorted access only to approved individuals (e.g., individuals who received a background investigation, including fingerprinting and a trustworthy and reliability assessment) through (1) the use of continuous physical barriers that allow access to the security zone through established access points, (2) direct control of the security zone by approved individuals at all times, or (3) a combination of continuous physical barriers and direct control (e.g., constant surveillance) (10 CFR 37.47(c)). Although the NRC allows direct control by approved individuals to be a method for securing the security zone, this section will primarily focus on the use of physical barriers to isolate, delay, and control access to risk-significant radioactive material (i.e., category 1 and category 2 quantities of radioactive material).

4.1.1 Continuous Physical Barriers

A continuous physical barrier limits access to the security zone only through established access control points (the fewer access control points the better). The continuous barrier should have no openings other than access control points large enough to allow a person to enter the security zone and to bypass the access control point. For example, a wall should be continuous from the floor to the structural ceiling, and openings (such as vents) that are greater than 96 square inches, where the smallest dimension is greater than 6 inches, should have metal grates, bars, expanded metal (i.e., an industry term for a screen made of steel or similarly strong metal through which an observer can see activities inside or outside an enclosure), or some other barrier that cannot be removed from outside the security zone. The licensee could use individuals (e.g., security guards) to control access points. However, using individuals to control access points may not be effective against adversaries that use force unless they are in a fixed and protected position and are properly equipped (e.g., armed) and trained on how to respond to an adversary attack.

A balanced protection approach should be taken for each aspect of the physical barrier configuration to enable equal delay between each part. For example, a blast-resistant door with high security locks at the access control point would not provide equal delay if the attached walls have a wood frame and are constructed of drywall. The design of physical barriers requires an understanding of the amount of delay that the material and hardware (e.g., locks, hinges, and bolts) for the walls, ceilings, doors, and windows will provide. A barrier is considered to be penetrated when a person can pass through, over, under, or around the barrier.

In addition, the licensee should use a delay-in-depth approach when designing the barrier system. Delay-in-depth means placing several different barriers in series (or in conjunction) rather than using one barrier. Different types of barriers will be susceptible to different attack methods. Therefore, each barrier may require the use of different types of attack tools and methods. Under such conditions, the adversary would need to be better prepared and to bring more tools to carry out his or her attack strategy. Requiring the adversary to bring more tools can cause a significant increase in the delay times, especially if he or she has to get through small openings or if the distance to the target area would require him or her to carry the tools for long distances.

The following items are examples of tools that an adversary could use to penetrate or bypass barriers:

- hand tools, such as sledgehammers, bolt cutters, and wrecking bars
- powered hand tools (e.g., electrical, hydraulic, pneumatic, or gasoline), such as drills, demolition saws, grinders, and jack hammers
- thermal cutting tools, such as oxyacetylene torches and plasma arc cutters
- explosives, such as bulk explosives, shaped charge, or thermite
- vehicles, such as trucks, cars, and sport utility vehicles
- heavy equipment, such as cranes, fork lifts, excavators, front-end loaders, and bull dozers

The licensee must ensure that all tools, vehicles, and heavy equipment located on site (inside or outside the facility) are properly secured so that an adversary cannot use them to bypass or breach the barrier(s) or use them to remove the radioactive material.

4.1.2 Walls, Floors, and Ceilings

Doors, windows, vents, and other conventional wall openings are generally the target for forcible entry because they are normally less resistant to penetration than walls. However, the proper tools (e.g., hand, power, or thermal tools, or explosives) can penetrate most structures (e.g., walls, floors, ceilings, and roofs). The amount of time needed to penetrate the structure depends on the type of material used and on the construction of the structure. Upgrades to existing structures or new designs can significantly extend the penetration time against hand, power, or thermal tools. For explosives, upgrading material thickness usually results in moderate penetration time; however, the amount of explosives needed increases greatly with the level of thickness.

The preferred type of material for use in the walls, floors, and ceilings of the security zone is concrete reinforced with rebar (e.g., 8 inches of concrete with two grids of No. 4 rebar). Reinforcement of concrete extends the penetration time needed for most tools (e.g., hand, power, or thermal tools). Explosives used on reinforced concrete will penetrate the concrete; however, the reinforcing rebar generally remains intact and, therefore, causes an adversary to use more time and tools before he or she can achieve entry. In addition, two or more reinforced concrete walls in series provide longer penetration delay times than one wall with a thickness equal to their combined thickness does. Penetration of multiple walls requires multiple individual efforts and the transport of tools through proceeding walls. If an adversary uses explosives, the contained internal pressure from the explosive charge could possibly collapse the ceiling and surrounding structures, thus creating further barriers in the form of rubble.

Other wall barriers used to increase the delay time could include earth cover or another type of overburden (e.g., vehicle barriers, such as concrete pylons or large rocks near walls on the exterior/perimeter wall(s) of the facility). In addition, thick or multiple layers of material (e.g., composite materials, such as concrete, cement, or expanded metal concrete) could be

used to extend delay times and to render an attack impractical because of the amount or type of tools needed to penetrate the structure. The licensee could also use a modular vault to specifically secure the risk-significant radioactive material. A modular vault is commercially available and is constructed from pre-manufactured panels that are generally made of high-strength concrete or composite. These vaults are assembled on site and can be designed to intimately contain the asset (e.g., risk-significant radioactive material or device).

4.1.3 Doors, Windows, and Other Openings

Doors, windows, and other wall openings are generally the weakest parts of a structure due to the design restrictions caused by their functional requirements and associated hardware. For example, facilities with thick concrete or brick walls, or both, provide access by the use of standard steel (e.g., hollow steel) or glass doors and windows. Using ordinary doors, frames, and hinges that an adversary can quickly penetrate basically negates the penetration delay time of the wall. The principle of a balanced design requires the strengthening of doors, windows, or other openings and their associated frames, hinges, bolts, and locks to afford the same amount of delay as that provided by the floors, walls, and ceilings of the structure.

For the room/area in which risk-significant radioactive material is located, the licensee should consider the following protective measures for doors, windows, and other openings:

- Limit the number of doors, windows, and other openings for the room/structure in which the facility uses or stores the risk-significant radioactive material.

- An adversary cannot lick door locks if the door-locking hardware/keyways are not exposed. For doors that do not need to be used as an entrance (only for exit), the licensee should consider removing external hardware and covering all external holes if safety and/or fire code requirements allow such measures (e.g., door opening hardware that is inside the room cannot be compromised from outside).

- For standard doors, adding steel plates to the surface of the door, using security door hinges that have a stud-in-hole feature, and grouting the door frame with concrete will strengthen the supporting structure of the door and will increase penetration time.

- Wood cores, especially redwood, placed between the door plates increases the penetration time for thermal cutting tools by a factor of 3 to 4 times that of a hollow door.

- To help prevent an adversary from prying open the door at the separation between the door lock and door frame, a strip of sheet steel can be welded or bolted to the door. This strip should be the same height as that of the door and should be at least 2 inches wide with a 1-inch overlap onto the adjacent door frame.

- Replacing a standard door lock with a high-security lock with a multiple deadbolt system or using door-intrusion sensors, or both, will mitigate lock vulnerabilities.

- For windows, the licensee should use glass glazing materials, such as laminate, Lexan®, or wire glass that is specifically meant for security applications (e.g., not just safety glass). For the window frame, the licensee should use additional or heavier fasteners or should consider welding the frame in place.

- A window that can open should have substantial fastening devices or should be replaced with a fixed window (i.e., a window that cannot be opened) if safety and fire code requirements allow such measures.

- For other openings (e.g., utility ports) and windows, the licensee should use metal grates, grills, steel bars, and expanded metal mesh and should consider reducing the size (e.g., dimensions less than 6 inches) of the opening to prevent the ability to crawl through the opening.

4.1.4 Locks and Locking Systems

Locks and locking systems are another important element for securing the security zone and risk-significant radioactive material. Locks are generally used to assist in controlling access to areas, facilities, and materials through doors, gates, container lids, and similar material or personnel access points. Although some locks are difficult to pick or manipulate, no lock can claim to be "manipulation proof." Therefore, the licensee should use locks in conjunction with other security measures, such as intrusion detection devices. In all applications, the licensee should ensure that the lock delay time and capability closely match the penetration resistance of the rest of the secured barrier (e.g., balanced protection). For example, the lock should not be significantly stronger or weaker than the attached door or wall.

The general types of locks that can be used to secure the security zone and risk-significant radioactive material are key locks, combination/padlocks, cipher locks, or electric locks. The best security practice is to avoid relying on keys to control access to the security zone. Key control becomes more difficult as time passes (especially for large institutions) as more duplicate keys are made for newly approved individuals. The same is true for the control of lock combinations over time. The licensee should use key cards, cipher locks, or some other type of electronic access control device where feasible instead of keyed or combination locks. Additionally, the licensee should ensure that each approved individual has a unique access code. With these devices, the licensee can delete the access code after an individual no longer requires access to the security zone or when a key card is lost or stolen.

The licensee should consider the following items when using key, combination, cipher, or electric locks:

- The licensee should select locks specifically designed for security applications, not common builder's hardware-type locks found in home improvement stores.

- For key locks, the lock should be capable of being set for a large number of different keys. (For example, the licensee should have enough keys for the number of people who will need access to the lock and should have extra keys for keys that are lost or for the turnover of personnel.)

- The licensee should ensure that the key cut required to open a lock is changeable so that a key can no longer be used when keys are lost or when an employee who has access to a key no longer requires access.

- A master-keyed locking system (i.e., using multiple locks that have one master key) should not be used for locks located within the security zone.

- Padlocks used to secure external barriers should be of rugged and sturdy construction and designed for outdoor use.

- If combination locks or padlocks are used, the licensee should use locks that meet Federal Specification FF-P-110J(1), “Padlock, Changeable Combination Lock (Resistant To Opening by Manipulation and Surreptitious Attack),” dated February 11, 1997.

- For controlling access, electric locks or electronic cipher locks are preferred because the exposed part of the lock is isolated from the part that contains the code, they offer versatility in programming (e.g., fairly easy change to combinations/access permissions), and they can be integrated into the alarm system (e.g., ability to prevent trial and error methods of surreptitious attack by activating an alarm after a number of unsuccessful attempts).

- The licensee should protect electric locks against tampering by using tamper switches that are connected to the alarm system.

In addition, the licensee should ensure that the locks are properly installed to protect the security zone and risk-significant radioactive material. It should consider the following factors when installing locks:

- The lock should be placed as far as it can from the face of the door, or a guard plate should be used that covers as much of the lock’s cylinder as possible (while still permitting the key to be turned).

- Special security screws should be used to mount security hardware located outside the secured area. The security screws should require a special tool for their removal, or they should not be able to be removed once they are installed (e.g., heads welded to the hardware/device).

- Screws that are used to mount a security device should also be hardened.

- If the lock or fastening hardware is mounted on wood, the licensee may achieve a higher level of protection by using screws that are long and strong enough to be embedded in the underlying structure (e.g., screws into wood framing or a concrete wall, or both).

Figure 4-1 Combination door lock with bypass key lock

4.1.5 Access Controls

Access control is also an essential function of the physical protection program. NRC regulations (i.e., 10 CFR Part 37.5, "Definitions") define access control as a system for allowing only approved individuals to have unescorted access to the security zone and for ensuring that all other individuals are subject to escorted access. The physical protection program should integrate access control measures that complement the implementation of other components, such as physical barriers and intrusion detection and assessment systems.

The first important function of the access control system is determining who is approved to enter the access control point. Licensees that use or store, or both, category 1 or category 2 quantities of radioactive material must have an access authorization program that complies with requirements in 10 CFR 37.23, "Access Authorization Program Requirements." Chapter 2 of this document provides information on the development and implementation of an access authorization program. The regulation at 10 CFR 37.21(c)(3) requires the licensee to ensure that only individuals whose job duties require unescorted access to category 1 or category 2 quantities of radioactive materials are approved for unescorted access.

After determining who should be approved for access, the licensee should have a system that can verify the identification of the approved individual. As a best practice, an identity verification system should use at least two of the following three factors:

(1) Require something that the person requesting access has in his or her possession (e.g., a credential).

(2) Verify something the person knows.

(3) Verify some characteristic of the person that can be measured.

Most identity verification systems use a credential (photo identification key card) to serve as something the person possesses. Using one or both of the other two factors mentioned above can help verify that the correct person is carrying that credential. A personal identification number (PIN) is generally used as something the person knows, and biometric devices are used to measure some characteristic (e.g., fingerprints, hand geometry, and eye pattern) of the person.

4.1.5.1 Coded Credentials

Many types of credentials can be used as part of the identity verification system. A photo identification badge is a common credential used for personnel access control. However, photo identification badges are not always effective because false photo identification badges can be made, or an individual can make up his or her face to match the face on a stolen badge to gain access. In addition, a photo identification badge generally requires a manual check by guard/security personnel; an inattentive guard can reduce the effectiveness of such a check, especially at times when a large number of people are entering an access controlled area. Coded credentials, which are also known as keycards, are the preferred type of credential to use as part of the access control system. Generally, coded credentials are in the form of a photo identification badge; the individual's photo and general information are included on a coded badge that can be read by a card reader that can grant authorized access (e.g., unlock door). Coded credential systems have a wide range of capabilities and can do the following:

- Eliminate the need for a manual check because the appropriate card reader system can automatically check an individual's authenticity.
- Assign a unique identification code number to the credential that can be read by a machine.
- Maintain entry authorization records for each coded credential.
- Terminate access authorization for an individual without the necessity to recover the individual's credential (e.g., key card).
- Assign different levels of access authorization, such as assigning access authorization to specific (i.e., not all) access control points or providing access only at certain times of the day.

Many techniques are available for coding a badge. The most common techniques include magnetic stripe, Wiegand wire, and smart cards. For additional information about coded credentials, see NUREG-1964, "Access Control Systems: Technical Information for NRC Licensees," issued April 2011.

Figure 4-2 Photo identification card with smart card

Card reader systems that read coded credentials work with both interior and exterior access control systems, and they generally work in conjunction with access control applications, such as door locks or gate-opening mechanisms. Card readers may be used in combination with numeric keypads for PIN entry, and they provide provisions for connecting to biometric devices. The access control panel of the card reader system generally has a range of input and output capabilities. For example, the access control panel can track the door status (e.g., open or closed) and can determine whether the door is being forced or attacked. In some systems, the panel can generate an audible alarm when the system is not accessed properly.

4.1.5.2 Personal Identification Numbers

Some access control systems allow the use of a PIN in addition to a coded credential or a biometric device to increase the level of security. These types of systems generally use the coded credential or biometric device to locate the reference file in the access control database that contains the PIN, and access is granted if the PIN that the individual enters on the keypad matches the pin associated with the reference file. When using a PIN, the licensee should ensure that the following minimum standards apply:

- The PIN should be a least four digits long.
- The user of the system should select his or her own PIN; however, the PIN should not be too meaningful to the user (e.g., not a birth date or partial phone number).
- No other system operator, security officer, technician, programmer, or other individual should be able to retrieve an individual's PIN.
- The access control portal (e.g., keypad) provided for PIN entry should minimize the opportunity for another person to observe the user entering his or her PIN.

- If an individual forgets a PIN, he or she should be required to reenroll in the access control system and select a new PIN.

- All users should be required to change their PINs at least annually.

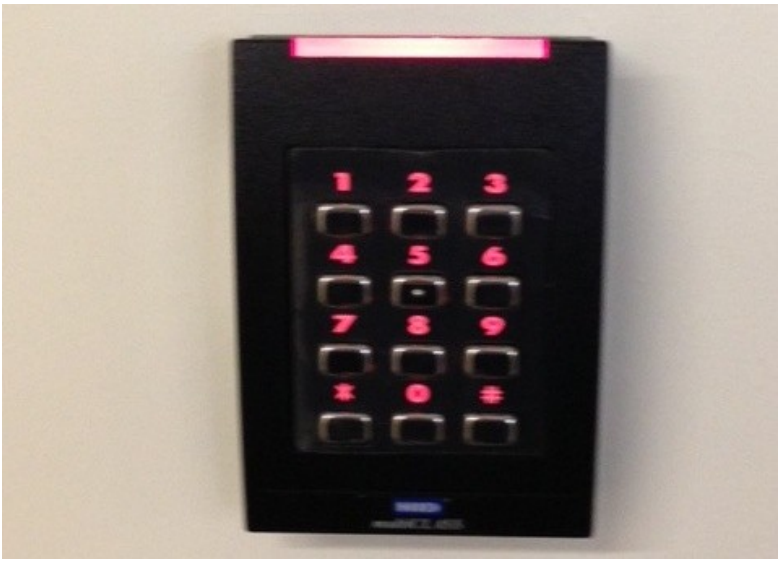

Figure 4-3 Card reader with associated PIN pad

Some systems provide a maximum number of attempts to enter the correct PIN before they reject the credential, generate an alarm to the monitoring station, or send out a duress notification. The duress capability in some systems can be built into the access control device by programming a specific PIN number for use as a duress code that is sent to the monitoring station. For example, a user may have his or her normal access PIN; however, he or she may also have a duress pin that will open the door and will covertly send a duress message to the monitoring station.

4.1.5.3 Biometric Access Control Systems

The term “biometrics” refers to systems that can measure specific physiological or behavioral characteristics of a person to aid in the process of identity verification. Biometric access control refers to the use of human biological attributes for verification or identification in physical or logical access control systems. Biometric devices can be based on any measurement of a human being. For the best performance, a biometric device should be based on a characteristic that is distinct, does not vary over time, and is easy to collect.

Biometric devices can serve as identity verification or identity recognition devices. Unlike passwords or PINs, the biometric-enrolled pattern cannot be shared or stolen. Therefore, the access control system can ensure positive verification or identification within the limits of its capability. For identity verification, the person initiates a claim of identity (e.g., coded credential) and presents the specific biometric feature for authorization (e.g., eye retina scan). If these items are in agreement, the equipment allows access. In identity recognition mode, the person does not initiate a claim of identity. The biometric device attempts to identify the individual; access is

only granted if the biometric information agrees with the information about the individual that is stored in a database.

The accuracy of a biometric device is usually described by its false accept and false reject rates. The false accept rate is the rate at which an imposter is improperly authenticated as matching a template that is based on another person's biometric feature. The false reject rate is the rate at which authentic users will fail to match their own templates. The licensee should test both the false accept and false reject rates when it first implements a biometric system to ensure that the system meets security performance requirements. The licensee should also establish a program to ensure that the system continues to function as intended and that regular maintenance and calibration are performed as required. Commercially available biometric systems normally operate with false accept and false reject rates of less than 1 percent.

Figure 4-4 Card reader with associated iris scan biometric device

When implementing a biometric system, the licensee needs to ensure that the facility has adequate space and resources for the enrollment station. The licensee also needs to ensure that the templates that are created during enrollment are protected and communicated to the access control system in a secure manner. A biometric device should provide a function that is complementary to the other systems and protective measures of a physical protection program.

The following considerations for biometric devices are critical:

- Accuracy. What are the false accept and false reject rates for the system in the given configuration?

- Throughput Rate. Does the system operate quickly enough to process the traffic entering the facility?

- Environment. Can the measurement be made accurately in the intended use location? For example, the system may be unable to acquire clear voice samples in a very noisy area or accurate facial images in areas in which sun glare can strike the individual's face during parts of the day.

- Database Access. How quickly can the template be retrieved from a central database? Some adaptive biometric systems adjust the template to account for human changes over time. How will the systems communicate these updates to the database and distribute them to other access points?

- Tamper Resistance. How well are the measuring devices protected from tampering? Are the electronics that perform the match and control door locks protected from tampering? Are all templates, databases, and communication lines protected from tampering?

Commonly available biometric systems are generally based on finger prints, hand geometry, facial image, voice patterns, and eye patterns. For more information about biometric access control systems, see NUREG-1964.

4.2 Monitoring the Security Zone

The regulations at 10 CFR 37.49, "Monitoring, Detection, and Assessment," require the licensee who possesses category 1 or category 2 quantities of radioactive material to establish and maintain the capability to continuously monitor and detect without delay all unauthorized entries into its security zones. In addition, the licensee must provide the means to maintain continuous monitoring and detection capability in the event of a loss of primary power or to provide for an alarm and response in the event of a loss of the capability to continuously monitor and detect unauthorized entry (10 CFR 37.49).

The use of an intrusion detection system is considered the best practice for continuously monitoring and detecting unauthorized entry into the security zone. NRC regulations allow approved individuals located within or outside the security zone to perform monitoring and detection of the security zone through direct visual surveillance (i.e., 10 CFR 37.49(a)(2)(iv) and 10 CFR 37.49(a)(2)(v)). However, the NRC does not recommend direct visual surveillance as the only or primary method used to detect an unauthorized entry into the security zone because, unless the individual is properly shielded and armed, the individual could be harmed or killed before he or she can notify anyone of the intrusion. Instead, the licensee should use direct visual surveillance as a temporary measure, such as when a temporary security zone that does not have permanent barriers at the boundaries is used or when the intrusion detection system is not functioning properly.

4.2.1 Intrusion Detection Sensors/Devices

The intrusion detection system (IDS) is an integral part of the physical protection program. Intrusion detection is defined as the detection of a person or vehicle attempting to gain unauthorized access into an area that is being protected. Detection of an intruder should take place as early as possible (before or at the delay barriers) to allow the response force enough necessary time to stop the adversary from achieving his or her final objective (e.g., theft or diversion of category 1 or category 2 quantities of radioactive material). Generally, intrusion

detection is accomplished by the use of sensors that, once activated, sends a signal to the monitoring station or activates an alarm, or both. Intrusion sensor performance is generally defined by the following three characteristic functions:

(1) probability of detection

(2) nuisance or false alarm rate

(3) vulnerability to defeat

The probability of detection for the perfect sensor is 1, which means that it always detects intrusion without fail. However, no sensor is perfect; therefore, the probability of detection is always less than 1. The probability of detection generally depends on the target under detection, the sensor hardware design, installation conditions, sensitivity adjustment, weather conditions, equipment condition, and acceptable nuisance alarm rate. The licensee should use a sensor with a higher probability of detection (e.g., close to 1) for protecting risk-significant radioactive material.

A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed but is not related to an intrusion attempt (e.g., animal/rodent or insects activating the sensor). A false alarm is an alarm generated without cause. Generally, false alarms are attributed to some type of electronic phenomena either by the sensor itself or the electrical infrastructure of the sensor system. An ideal sensor would have a nuisance or false alarm rate of zero; however, all sensors interact with their environment, and they cannot tell the difference between adversary intrusions or other events that may cause their activation. For this reason, detection is not complete without assessment. Detection begins with sensor activation and ends with the conduct of an assessment to evaluate the cause of the alarm.

Note that all sensors can be defeated. Different types of sensors and sensor models have different vulnerabilities. An intruder can defeat a sensor either by bypassing the sensor or spoofing the sensor. An intruder can bypass a sensor by going around its detection zone/volume. Spoofing is any technique that allows the intruder to pass through the sensor's normal detection zone without generating an alarm. Understanding the vulnerabilities that a sensor may have allows the licensee to establish other compensatory measures to compensate or remove the vulnerability (e.g., a complementary sensor is used or measures are taken to limit an intruder's ability to bypass the sensor).

Another factor that should be considered when choosing the type of intrusion sensor is whether an active or passive sensor would work best for the specific area that is being monitored. Active sensors transmit a signal from a transmitter, and a receiver detects changes or reflections of the signal. Passive sensors do not produce a signal. They are basically receivers that detect energy that is near the sensor. Note that the presence or location of a passive sensor can be more difficult to detect than that of an active sensor because a passive sensor does not emit a signal or energy that an adversary could possibly detect.

This section provides a general overview of the types of intrusion sensors that can be used to detect an adversary. For detailed information on intrusion sensors, see NUREG-1959, "Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees," issued March 2011.

4.2.1.1 Sensors Used for Doors, Walls, and Utility Openings

Magnetic switches are commonly used passive detection sensors for doors, windows, or other utility openings. Most residential and small business security systems use the simple magnetic switch. However, little knowledge is necessary to defeat (bypass or spoof) a simple magnetic switch. A balanced or bias magnetic switch (BMS) is the preferred device to use for doors, windows, and other openings within the security zone. The BMS is much harder to defeat than the simple magnetic switch is. Because the newest switches on the market have very narrowly defined magnetic field paths, they are almost immune to external magnets that can be used to defeat the switch. BMS sensors are also very reliable when they are installed correctly on a properly installed door with hardware that is in good condition. In addition, the activation of nuisance alarms is almost never caused by the BMS alone.

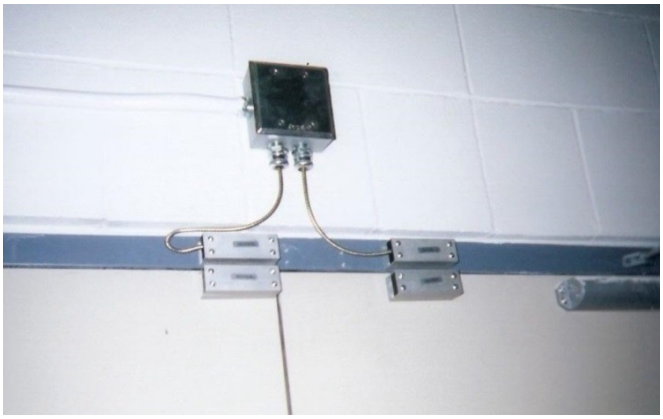

Figure 4-5 Triple-biased BMS sensor on double doors

A glass-break sensor is a passive sensor that detects when a pane of glass is broken or shattered. Glass-break sensors usually use a microphone that monitors frequencies or vibrations from the glass. If the frequency or vibration exceeds a specific threshold (that is sometimes user selectable), an alarm/signal is activated. Glass-break sensors are generally more susceptible to having a higher nuisance alarm rate. More complex designs compare the sound analysis to one or more glass-break profiles and react if both the amplitude threshold and statistically expressed similarity threshold are breached. These more complex designs cost more; however, they have a lower nuisance alarm rate. Glass-break sensors should be used as secondary sensors (e.g., in addition to a BMS or motion sensor) because they have a higher nuisance alarm rate.

Figure 4-6 Glass-break sensor

The licensee should consider doors (entry/exit ways) required for use as emergency exits (i.e., required by fire codes) as a vulnerability that should part of the intrusion detection system. An emergency door generally should have a single-hand/single-motion exit device. Additional security measures should be taken when the emergency exit doors located in the security zone have controlled entrance and free exit or egress. One measure that can be taken is to add a request-for-exit sensor at the door. This infrared (IR) sensor detects a person approaching the door from inside the security area and can send an alarm that the door is about to be opened. An additional measure that can address fire code requirements while maintaining secure control includes the use of delayed exit hardware in which the door can be opened only after a short period of wait time. This method allows the use of video cameras to assess the activity at the exit.

4.2.1.2 Motion Sensors

Motion sensors, or volumetric sensors, allow the licensee to detect motion within the whole volume or a portion of the volume of a room or building. An advantage of using motion sensors is that they can detect an intruder moving in the detection zone regardless of his or her point of entry into the zone. Several different types of technology fall under the category of motion sensors, such as microwave, IR, ultrasonic, dual technology, and video motion detection. The type of sensor used should depend on how the characteristics of the sensor best match the environment or possible vulnerabilities, or both, in the area being monitored.

Microwave sensors are active sensors that use a single antenna for both the signal transmission and receiving function. Motion within an area monitored by a microwave sensor will cause changes to the microwave energy, and these changes are a type of Doppler frequency shift. A person or other object moving within the microwave energy field will cause minute changes in the frequency of the microwave. An alarm will be generated if the frequency difference exceeds a preset threshold (a threshold generally set by the user). Microwave sensors are most sensitive and effective when they are installed in such a manner to necessitate an adversary walking toward or away from the sensor.

Microwave sensors can be used to effectively monitor interior confined spaces, such as vaults, special storage areas, hallways, and service passageways. They can also serve as an early warning alert of intruders approaching a door or wall.

Because of the high signal frequencies of microwave sensors, the signal/sensor is not affected by moving air, changes in temperature, or humidity. However, the high frequency allows the signal to pass through standard walls, glass, sheetrock, and wood, which can cause the activation of nuisance alarms through movement adjacent to, but outside, the detection area. The structural materials and the thickness that a particular microwave can penetrate will vary based on the device's manufacturer, model, and frequency.

The licensee should consider a complementary or second sensor, such as a passive infrared (PIR) sensor, to further enhance detection within an area that uses a microwave sensor. The use of a complementary sensor provides a second line of defense and provides security personnel additional information to help them accurately assess an alarm and to discriminate actual or potential penetrations from nuisance events.

PIR sensors are the most commonly used volumetric sensor for interior applications. PIR sensors detect the electromagnetic-radiated energy generated by sources that produce temperatures below that of visible light. PIR sensors do not emit any energy field into the area that they are monitoring and do not measure the amount of IR energy. Instead, PIRs measure changes in thermal radiation by sensing the change in contrast between a heat source and the ambient background temperature. A PIR sensor is complementary to a microwave sensor because a PIR best detects an adversary when he or she moves across the zone of detection, whereas the microwave sensor detects movement directly toward or away from the sensor.

Any object causing an appropriate temperature differential can potentially generate a nuisance alarm in a PIR sensor. Rapid changes in localized heating and cooling can cause the required temperature differential. The following factors may affect these changes:

- sunlight
- incandescent light bulbs
- radiators
- space heaters
- heating, ventilation, and air conditioning vents
- hot pipes

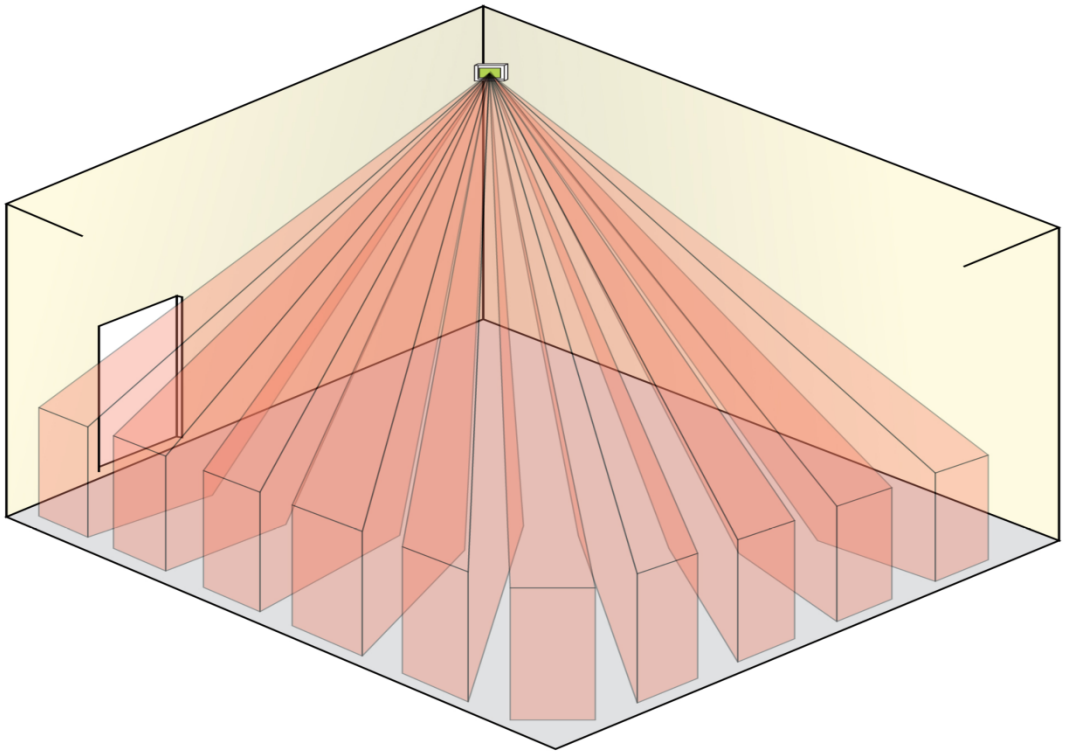

Figure 4-7 PIR sensor detection pattern (Note that a specific number of segments must detect an anomaly before the sensor will signal an alarm condition.)

In practice, localized heating and cooling are less likely to activate nuisance alarms because temperature changes generally do not happen rapidly. The licensee should remove or shield all hot spots that generate IR energy when using PIRs. Radiant energy from such sources may produce thermal gradients that change the background energy pattern. Ultrasonic sensors are similar to microwave sensors because detection is also based on the frequency shift between the transmitted and received signals caused by the Doppler effect from a moving object. However, ultrasonic sensors use energy in the acoustic spectrum, which is at a lower frequency than that of microwave sensors; therefore, these sensors do not penetrate solid materials, such as walls, cardboard, and windows. Because the ultrasonic energy will not penetrate physical barriers, the walls of the room will either absorb or reflect the energy. Generally, most walls will reflect the ultrasonic energy, which will help fill the detection zone and thus make it more difficult for an intruder to escape detection by an ultrasonic sensor. Note that large objects (e.g., bookcases and desks) located in the detection zone of the sensor could create shadow zones, which can cause detection problems. However, this can be overcome by using multiple ultrasonic sensors to cover the volume within the area.

Dual technology sensors are another type of sensor that are primarily designed to lower the false or nuisance alarm rates in an interior sensor. Combining two different types of sensors (e.g., microwave and PIR) in one casing or unit so that each sensor is complementary to each other (i.e., each sensor generates a different set of nuisance alarm sources) lowers the false or nuisance alarm rate. Generally, the two sensors are connected electronically by using an “AND” gate logic function in which both sensors must sense an event within a predetermined time interval (e.g., a few seconds) before a valid alarm will be generated. The time interval is usually a parameter that the user can configure.

Figure 4-8 Dual technology sensor

Reducing the nuisance alarm rate of a sensor is highly desirable; however, making a sensor less sensitive to possible nuisance alarms also makes it less sensitive to valid alarm conditions. Unfortunately, two different types of sensors are not likely to both be optimally installed in the same location. For example, a PIR sensor would be best positioned in such an orientation that an adversary would likely walk across the detection zone of the sensor, whereas a microwave sensor would be best positioned in such an orientation that an adversary would likely walk toward or away from the sensor. Because of this possibility, the licensee should not use dual technology sensors configured to operate in an "AND" gate logic unless it can establish an optimum location that would provide a high probability that both sensors would be able to detect the adversary. The installation of two different types of sensors in locations that are optimal to their own detection capabilities would be better than using dual technology sensors.

Video motion detection (VMD) is another type of passive sensor that can be used with either analog or digital camera systems. VMD has been effectively implemented using daylight cameras, near IR cameras, thermal, or alarm processing hardware and software. The technology is modular for implementation at either the camera or at the alarm monitoring station. In one configuration, VMD software can be downloaded into specifically configured digital cameras with embedded digital signal processor (DSP) chips and memory to enable the camera to perform the detection function. When a VMD detection event occurs (e.g., movement occurs in the camera's field of view), the camera sends an alarm message to the monitoring station. Prealarm video can also be stored in the digital camera's memory, and then the DSP transmits it to the monitoring station or monitoring device (e.g., e-mail to smartphone) when an alarm event has occurred.

VMD technology has experienced significant advances since the early 2000 timeframe. Lower performance modules are available that provide simple movement detection, whereas higher performing equipment uses sophisticated algorithms to detect and categorize a moving target. VMD functionality is generally available in the following three configurations:

- software running on a personal computer with video capture cards.
- standalone single- or multiple-channel hardware/software modules
- software embedded within a digital camera with an onboard DSP chip and associated memory

VMD technology that is used indoors where environmental variables are significantly fewer produces significantly fewer nuisance alarms. Indoor lighting in most locations is fairly constant throughout the day, and generally the camera-to-target distance is much shorter than that encountered in outdoor applications. Cameras tend not to shake and vibrate in indoor applications, and animals are usually not present to trigger alarms.

Figure 4-9 Example of a VMD camera

Combining the use of VMD with assessment cameras in indoor applications provides sensor functionality without the use of a separate physical sensor. However, the camera and VMD software cannot sense the presence of an intruder within a sensored space. Changing attributes of a video image are analyzed by software, and the results of that analysis determine whether an alarm condition is present. Current video analysis software only approximates a portion of the detection and assessment capability of the human mind. Although VMD detection software has significantly improved, it is definitely not superior to human visual acuity and cognition. However, VMD software does provide surveillance 24 hours a day/7 days a week to respond to predefined targets and attributes of movement within a scene. Humans do not have the capability to continuously focus on a scene for extended lengths of time. VMD provides that continuous observation and alerts the monitoring station or individual to allow him or her to make the final decision on the presence of an intruder.

4.2.1.3 Proximity Sensors

Proximity sensors, or point protection/detection devices, have the capability of detecting someone approaching, touching, or attempting to remove valuable items, such as devices that contain risk-significant radioactive material (e.g., self-shielded irradiators and medical therapy devices). Proximity sensors usually form the inner most level of detection to the asset (e.g., after boundary penetration sensors or volumetric/motion sensors, or both). Because these sensors are usually located close to a particular asset (e.g., category 1 and category 2 quantities of radioactive material), the response force has the least amount of time to respond to an alarm once the intruder is detected.

Therefore, the licensee should not use proximity sensors as the primary means of detection on high-risk items. Proximity sensors are most effective for detecting threat from an insider.

The primary types of proximity sensors include capacitance, pressure, strain, and switches. Capacitance proximity sensors operate on the same principle as an electrical capacitor. These types of sensors are generally used on metal containers that can be isolated from ground, such as safes or shielded devices that contain radioactive material (e.g., self-shielded irradiator). An electrical capacitor comprises one or more conductors separated by a dielectric medium. A change in the electrical characteristics of the dielectric medium causes a change in the capacitance between the two plates. In the case of the capacitance proximity sensor, the metal object corresponds to one plate and an electrical reference ground plane under or around the protected object corresponds to the second plate. An insulator isolates the protected object from ground. The air between the object and ground comprises the dielectric medium. When a person comes close to the object or touches it, the dielectric is changed, which then changes the capacitance. The processor (part of the capacitance sensor) detects the change in capacitance and generates an alarm. The sensitivity of capacitance sensors is affected by changes in relative humidity and the relocation of other metal objects closer to or farther away from the item. If the sensitivity is increased, the chance for nuisance alarms increases. If the sensitivity is lowered, detection capability is lowered.

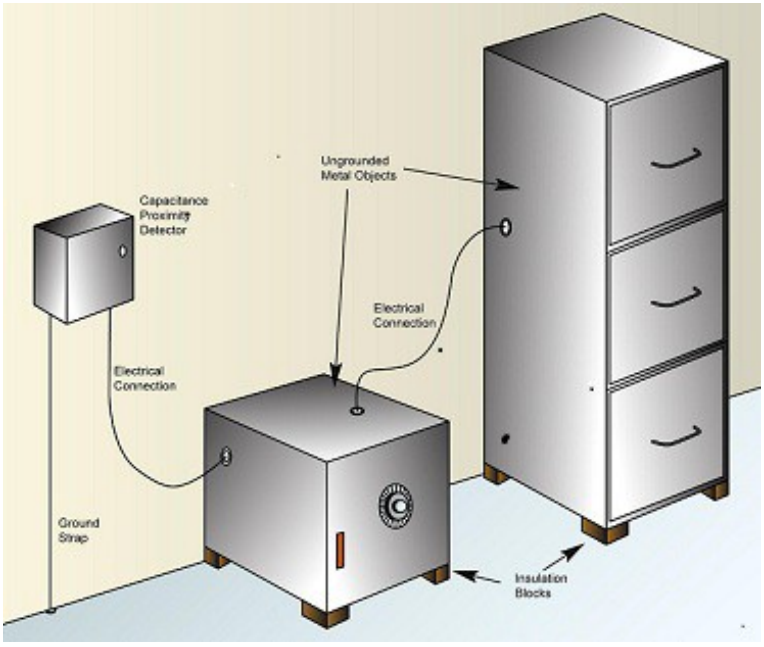

Figure 4-10 Example of a capacitance sensor installation

Pressure sensors incorporate a sensing device that responds to deformation of the sensor caused by the placement of weight on it. Generally, a pressure mat is used that consists of a series of ribbon switches positioned parallel to each other, approximately 3 inches apart along the length of the mat. Ribbon switches are constructed from two strips of metal in the form of a ribbon separated by an insulating material. They are constructed in such a manner to allow the metal strip to make electrical contact when an adequate amount of pressure (depending on the application) is exerted anywhere along the ribbon. They can be used to detect the presence of intruders when they approach or attempt to move protected items. For instance, pressure mats

can be installed under the carpet around the protected item. Anyone who approaches the item must step on the mat, thus initiating an alarm. The pressure sensor output signal is routed to an alarm console to indicate an intrusion. Nuisance alarms from pressure sensors can occur if the insulating or separating material that keeps the ribbon switch contacts apart deteriorates because it is worn out or exposed to harsh conditions. Extreme heating and cooling (out of the operating range) are additional nuisance alarm sources, especially if the mat is worn and deteriorated.

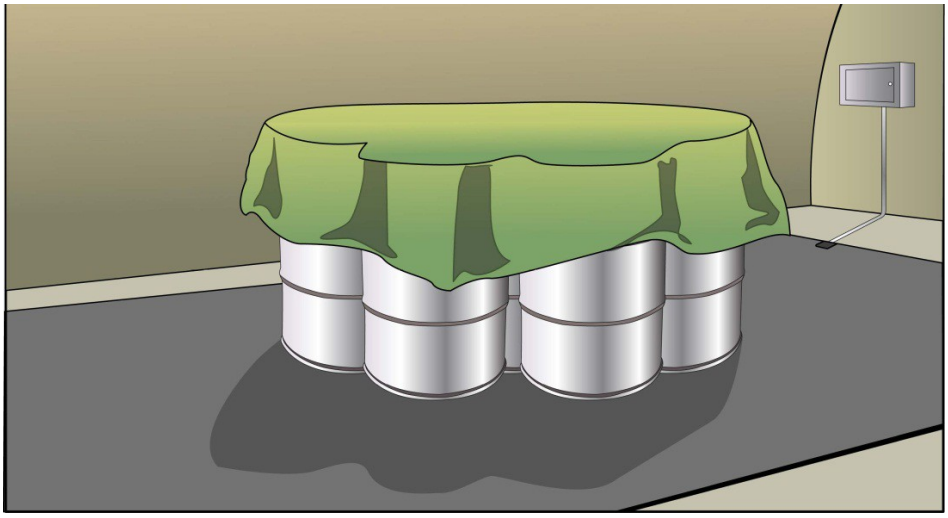

Figure 4-11 Example of a pressure mat

Strain sensors measure small amounts of deformation or flexing of a surface. A basic configuration of a strain sensor would be one or more sensing devices connected to a processor. The sensing devices can employ metal foil or wire to detect surface deformation or flexing. When configured to be a strain sensor, the electrical properties (such as resistance) of these materials will change when they are bent, stretched, or compressed. The processor continually measures the electrical properties of the sensing device and will activate an alarm or another indication when a specified amount of change has occurred. Processors will typically have user programmable controls to specify how much change has to occur to activate an alarm. Changes in temperature or humidity can affect strain sensor device and thus activate nuisance alarms. The licensee can configure some strain sensors to reduce or eliminate the effects of temperature changes.

Switches can be used as a proximity point sensor. A protected item is placed on the switch, actuating it so that the electrical contacts are either in an open or closed position. Alarm system electronics monitors the switch for a change in the position of the contacts. If the item is removed, the contacts change position and an alarm is generated. Movement of the item can also generate an alarm if the type of movement causes the switch contacts to change positions. The design of the surface and switch mounting should make the removal of the asset while maintaining the switch in the secured position difficult. Switch sensors that are in good condition and installed properly should have very few, if any, nuisance alarms. Primary nuisance sources include loose or damaged mounting brackets, fasteners, and mounts and damaged or worn out internal or external components of the switch itself.

4.2.1.4 Duress Alarms

A duress alarm is an alarm that is manually activated by an individual. This alarm should indicate that an individual has detected or is experiencing some type of an event. (For example, the individual sees an unauthorized individual in the security zone.) Devices/buttons (e.g., panic buttons) that activate duress alarms should be located in areas outside and inside of the security zone. These devices can be covert (hidden) or visible. The licensee should be careful when positioning these devices to avoid their inadvertent activation. The security plan or procedures, or both, should include information on the location and use of these alarms, and the licensee should provide training to individuals who may be required to use these alarms.

4.2.1.5 Radiation Detectors

Radiation detectors can be used to detect the movement/removal of risk-significant radioactive material. A radiation detector may already be located within the facility as a safety feature (not security-related feature). The radiation detectors used for safety should not be used for security functions because the safety purpose will be different from the security purpose (e.g., a detector used to check for contamination versus a detector used to indicate that an intruder is removing radioactive material from the security zone).

A radiation detector for security purposes should be located in a specific location and should be able to send a signal to the monitoring station(s) indicating that there is radiation that would not be normally present unless the risk-significant radioactive material has been, or is in the process of being, moved (e.g., no longer shielded). In addition, to mitigate the threat of an insider, the radiation detector should be separate from the security zone alarm system, should always be armed with no ability to disarm it, and should be able to send a separate (e.g., different from the security zone alarm system) signal/alarm to the monitoring station(s). Note that the radiation detector that is used should be appropriate for the type and amount of radiation emitted from the radioactive material that is secured. Generally, the Radiation Safety Officer for the facility should assist in determining the appropriate detector to use and in explaining how to properly set the detector to detect the possible radiation from the source (e.g., set the detector to alarm at radiation levels above background or some other specified value). Note that most radiation detectors need to be routinely checked for operational response with an appropriate check source that contains radioactive material. The licensee may need license authorization to possess certain check sources. In addition, the licensee must periodically calibrate the radiation detectors as specified by the manufacturer of the detector and should ensure that the calibration is done by the instrument manufacturer or a person specifically authorized by the NRC or an Agreement State. Licensees can calibrate their own instruments if properly authorized for that activity.

4.2.1.6 Exterior Intrusion Sensors

Exterior intrusion sensors are used in an outdoor environment to detect a person or vehicle attempting to gain unauthorized access into a protected area. This chapter primarily focuses on interior security of the facility (e.g., security zone). However, licensees should also consider the use of exterior intrusion sensors to enhance the level of protection for the facility by providing the means for earlier detection to allow for a longer response time to stop the adversary. NUREG-1959 provides detailed information on exterior intrusion sensors.

4.2.2 Alarm Communication and Display

The primary objective of a physical protection alarm system is to communicate alarm events received from sensors to an individual. An effective system should be capable of operating under all conditions and continuing to operate even when individual components or primary data communication paths fail. This type of failure is the reason that redundant data communications capabilities are important. The goals of the system are to report alarms in a timely manner (never lose alarms) and to survive any single-point failure with minimal or no degradation in system performance.

In general, alarm communication and display (AC&D) systems should have the following capabilities:

- A data communication subsystem should move alarm data in a timely manner. Alarms should communicate to the onsite and offsite alarm monitoring station immediately. The data communication subsystem needs to be fast enough to allow the overall alarm system to meet these times. Alarm timing is measured starting at sensor activation and ending at alarm display (visual and audible) to the monitoring station or individual.

- If an offsite alarm monitoring station is used, the monitoring station should be a monitoring station approved by Underwriters Laboratories, Inc. (UL), that can receive the alarms, assess the situation immediately, and dispatch the response force. A UL-approved monitoring station means that the monitoring station is using UL-certified equipment that meets the minimum standard for alarm-monitoring operations.

- The data communication system should be robust with no single-point (e.g., single location) failures between sensors and the alarm stations. Single-point failures are defined as the loss of the entire, or a significant portion of the, detection and assessment system capability through the loss of any single critical component/communications link (e.g., a single phone line with no line failure detection). The failure of a critical component/communications link within the AC&D system would completely or significantly degrade the detection and assessment capability of the security system and would require approved individuals (e.g., security force or authorized users) to replace the functions of detection and assessment to maintain security system effectiveness. Intrusion detection and assessment systems should have no single component link or location that, if it fails, would degrade the continued detection and assessment capability of the remainder of the system.

- The system should be designed with redundant data communication links. “Redundancy,” which refers to the ability of the system to complete the same task through multiple means, is recommended between sensors and the alarm monitoring station.

- The alarm system and associated data communications systems should not lose any intrusion or entry control alarms, events, tamper alarms, state-of-health messages (AC&D system status), or any other alarm necessary to meet the level of protection of the system design.

- The system should automatically notify the monitoring station when components of the intrusion detection and assessment system fail. This status monitoring should be continuous, and any faults should be reported to the monitoring station immediately. In addition, the system should notify the monitoring station when components return to proper operation.

- The data communication system should be highly reliable with minimal downtime for repair or maintenance.

- A malevolent or attack will generate many intrusion detection alarms simultaneously. The system should be able to handle malevolent situations without failing and without losing any of the multiple alarms. The system should be able to handle up to eight simultaneous alarms and should be able to count and display the number of unacknowledged alarms upon receipt of those alarms. The system should display the first alarm received and should indicate the number of remaining alarms.

- The system should be designed to provide automatic "failover" to the greatest extent practicable to enable continued detection and assessment when single components, communication links, or locations fail. "Failover" refers to the ability of one resource to switch to another resource if one component fails (e.g., the central processing unit (CPU) for the onsite monitoring station "fails over" to an alternate CPU located at another location (e.g., an offsite monitoring station).

- Upon restoration of failed equipment or data communication links, the system should return to its original state within 30 seconds. No alarms should be lost while the system is returning to its original state.

- Upon system restoration, the system should be capable of sustaining another failure at a single physical location while still maintaining its capability to perform as designed.

- The periodic testing and maintenance of alarms and associated systems should be performed at the manufacturer's recommended timeframes or minimally at least every 12 months.

4.2.2.1 Line Supervision

Line supervision is the means for monitoring the communication link between a sensor and the alarm reporting system (e.g., monitoring station). Use of supervised lines between the sensor and the alarm monitoring station and continuously monitored sensor tamper switches will help mitigate an insider threat. The licensee should be familiar with the range of line supervision techniques that are available for the communication lines that connect a sensor alarm relay to the alarm reporting system. Alarm communication systems should continuously detect failures of, and tampering with, critical components associated with alarm detection, transmission, and annunciation. Events should be immediately reported to the monitoring station.

Note that the NRC requires the licensee to provide an alarm and response in the event of a loss of the capability to continuously monitor and detect unauthorized entries

(i.e., 10 CFR 37.49(a)(1)). The licensee could not achieve continuous monitoring and detection if the alarm system or alarm monitoring station, or both, cannot notify the licensee and response force immediately upon an alarm communication line failure. Generally, the monitoring station interrogates or checks the alarm communication lines (e.g., pings the line) to ensure that the communication system is working properly. However, not all monitoring stations interrogate the line continuously. (For example, the line may only be checked once every 4 hours or less.) The licensee should verify or request that the alarm monitoring station continuously (e.g., every second) interrogates the line, and the monitoring station should immediately notify the licensee and the response force (i.e., local law enforcement agency (LLEA)) if the interrogation of the line indicates an interruption in the line (e.g., communication with the sensor fails). The licensee should understand how often the alarm monitoring station interrogates the line and should understand the process for notifying the facility and the response force when a communication line fails.

All computer security networks used for physical protection systems should be dedicated solely to security operations. The computer security network should not be connected to the Internet or any other local or wide area networks that are not related to security. When communicating between remote sites (sites that are not part of the internal data communications), the licensee should ensure that all data communications are encrypted to the level corresponding to the sensitive unclassified or classified nature of the data communications. The licensee should also ensure that all system components are protected against tampering and unauthorized manipulation. Detection, assessment, and access control devices that communicate using radiofrequency signals are not recommended because these signals can be interrupted or jammed and thus inhibit equipment performance.

To protect the system from unauthorized manipulation (e.g., hackers or others who have malevolent intent), the licensee should not connect a security local area network, if used, to any external computer network. However, for associated access control systems, the standalone system could allow (through firewalls and other information technology equipment) temporary or one-way connections to external networks to import badge information that is encrypted. System developers need to protect and secure communication equipment and media against unauthorized access. Equipment cabinets containing alarm communication equipment should employ tamper alarms (e.g., proximity sensors) to achieve this function.

4.2.2.2 Alarm Display

Current AC&D systems use both text and graphic displays to uniquely identify alarms to a monitoring station operator. Many types of information can be displayed; however, some of the more important information includes the following:

- mode of any sensor[1]
- status or state of an event[2]

---

[1] "Mode" refers to the status of a sensor. Is the device being monitored or ignored? Is the sensor online or offline? Other standard terminology includes "access" or "bypass," which means the same as "offline."

[2] Alarm status (state) can include "alarming" (detecting) or "secure" (no detection).

- time of events
- location of events

At a minimum, the monitoring station console should display the following information for alarm events:

- visual and audible annunciation of the alarm
- alarm type (intrusion, duress, or tamper alarm)
- alarm location
- time of alarm
- site-specific sensor identifier (a minimum of 64 characters)
- sensor state (alarm, secure, or tamper state)
- sensor mode (access, secure, or offline mode)

Configuring the system to meet the needs of the site or facility is important. The system should be flexible. For example, users should be able to configure the system to direct a particular alarm, tamper, or system event to the desired console. The system should be able to direct an event to more than one console (e.g., send all intrusion alarms to the onsite monitoring station and the offsite monitoring station). System administrators of the system should be able to direct alarm events to consoles based on their location, priority, or sensor type.

4.2.2.3 Alarm Prioritization

Some intrusion detection events, such as intrusion alarms and tamper alarms, are considered to be of higher priority than that of other system events. In some cases, alarms received from specific intrusion sensors may be considered of higher priority than that of others. The system administrator should assign priority levels to system events within the system, consistent with the facility's protective strategy and the objectives of the physical protection program. The system software should not make assumptions or place constraints on the priority assigned to a particular event. The system must be able to prioritize the display and to handle system events that include, but are not limited to, the following:

- intrusion alarms from interior or exterior sensors
- equipment tampers
- system faults
- data communication system faults, failures, or tampers
- duress alarms

- alternating current power loss
- access control alarms and events
- low battery alarms

Prioritization of system events is a site-specific decision. The licensee should make these decisions after considering the elements of the physical protection program, the site's protective strategy, and the geography of the site. The AC&D system should allow events to be assigned a priority based on location or event type; however, exact priority assignments are site decisions.

The system should automatically handle the organization of incoming events. Normally, system events are displayed in order of priority and then by time of arrival. System administrators should be able to assign the same priority to different events. (For example, all alarms and tampers may have the same priority.) In addition, the system should allow flexibility to handle any event that is out of priority order.

4.2.2.4 Alarm Logs and Reports

Alarm logging lets the system maintain an historical record of alarms so that alarm station operators, system administrators, or other approved individuals can access a list or log of all system events and activity. The AC&D system should have the capability to export system log files into commonly used file formats for reporting or analysis. The alarm log should provide a record of all alarm events and all system events. The alarm log should include other useful information, including the following:

- time of operator acknowledgment
- a "tagging" ability so that the operator can tag an alarm event with its cause
- time of an operator cause assessment (completion of operator action)

The system should also be capable of producing reports of alarm activity and providing the numbers and types of alarms based on their cause or location. The following examples are beneficial reports used to evaluate the continued health and maintenance needs of the system:

- Nuisance and false alarm reports detail the total number of alarms, false alarms, and nuisance alarms per sensor zone (location), for a user-selectable time period.
- Sensor grouping reports are based on the types of sensors or their location. In particular, these reports are useful for interior sensors and exterior sensors.

To avoid tampering by an insider, the system should prevent individuals (e.g., monitoring station operators) from deleting saved events. In addition, the system should be designed or programmed to ensure that an alarm station operator or system administrator cannot change the status of a detection point or deactivate a locking or access control device without the knowledge and concurrence of another approved individual, such as the security manager.

The AC&D system can help monitoring station operators and administrators by incorporating several other automated features and capabilities. For example, a good AC&D system can provide capabilities for logging events and saving them; when the log is full, the system should provide an archive capability that will save the information in a long-term storage medium. If the alarm reporting log or storage space (such as a hard disk) becomes filled to capacity, the system should not fail or lose information or degrade its performance. The following system capabilities may apply:

- The system could incorporate automatic notification (such as an e-mail to the administrator) when the log space becomes limited. An "alarm log full" report can be generated at helpful intervals, such as 80 percent full, 90 percent full, and 95 percent full. Users can archive the log files before any information is lost, or new information cannot be added.

- The system can incorporate an archive capability to move the log information to removable media, such as compact disks or digital video disks (DVDs).

4.2.3 Emergency and Backup Power

The primary power source for critical security systems and components should come directly from the normal onsite power distribution system or directly from the public utility. Because of the potential for a loss of power caused by a natural phenomenon, such as weather, or by a malicious act committed by an adversary, a facility should have reliable backup and emergency power sources on site that will provide power when needed. Facilities should have backup power that will last long enough to establish contingency measures (e.g., approved individuals to maintain constant control and surveillance of the security zone). Note that licensees located in areas that are more prone to frequent or long-term power outages (e.g., coastal areas) should have contingency plans to address long-term power outages, especially in the cases where they may need to hire additional personnel to help secure the security zone.

All critical security systems and components, including the following, should have an emergency/backup power capability in case they lose primary power to function as intended to maintain a high physical protection standard:

- intrusion detection equipment

- assessment equipment (e.g., closed-circuit television systems)

- illumination equipment (i.e., lights required for assessment cameras)

- automated access control systems

- alarm monitoring systems

- nonportable communications equipment

These power sources should contain an automatic switching capability to the auxiliary source of power (battery or generator, or both) that will function immediately without causing false alarms and without causing a loss of security system function or data. The licensee should design the alarm systems to enable the responsible parties to automatically receive an alarm signal indicating any of the following conditions:

- The primary power source has failed.
- The facility has transferred to an emergency/backup power source.
- The emergency/backup power source has failed.

In the design and selection of an emergency/backup power source, consideration should be given to site-specific conditions for the capability to restore primary power. The capability of the emergency/backup power source to sustain security system operations should be based on the timeframe to restore primary power.

The following three primary emergency/backup power categories are used:

(1) uninterruptible power supply (UPS)

(2) batteries

(3) engine generators

A UPS is an electrical device that contains internal batteries that provide a continuing source of power usually for a short period of time. UPSs are typically used to supply an uninterrupted source of power to important instrumentation and control systems to enable continuous operation during the loss of normal power without the loss of system or component functionality. They also provide continuous quality power to systems that are sensitive to disturbances in an electrical power distribution system caused by switching, faults, or power transfer. Most UPS systems are placed between the primary power source and the component that they protect so that they can effectively funnel all power at all times while keeping their own batteries charged.

A battery backup system should include all switchgear (i.e., equipment that switches primary power to the backup power) and distribution equipment (i.e., equipment that distributes the backup power to applicable components) necessary to provide quality voltage and current as required by the connected load. The batteries are normally in full float operation, whereby (1) they are connected in parallel with a charger and (2) the load and the charger supplies the normal direct current load plus any self-discharge or charging current, or both, required by the battery.

An engine generator is a device that converts mechanical energy to electrical energy generally through electromagnetic induction. For most industrial applications, a diesel engine supplies the mechanical energy. When an engine generator is properly sized and designed, it will provide reliable electrical power to the intended load equipment for the required amount of time. An engine generator should be capable of providing power compatible with the equipment it sources. The generator should have adequate capacity and rating to enable the operation of all loads

simultaneously. The emergency/backup power system should start automatically (or be brought online) upon loss of primary power.

A UPS or an engine generator, or both, are typically the best type of emergency/backup power systems for use in the security system. A UPS used in conjunction with an engine generator is the most effective power method available because of the ability of the UPS to continuously operate the critical components without interruption and because of the ability of the engine generator to sustain power for a longer period of time.

The licensee must understand the capability of the emergency/backup power system and must know how long emergency/backup power will last and what systems are being backed up. Because of the nature of emergency/backup power supplies and because of their expected irregular schedule of use, regular maintenance and testing is critical to guarantee their full functionality and reliability when the primary power source is unavailable. The licensee must ensure that it is performing the manufacturer's recommendation for the maintenance and testing of the emergency/backup power system.

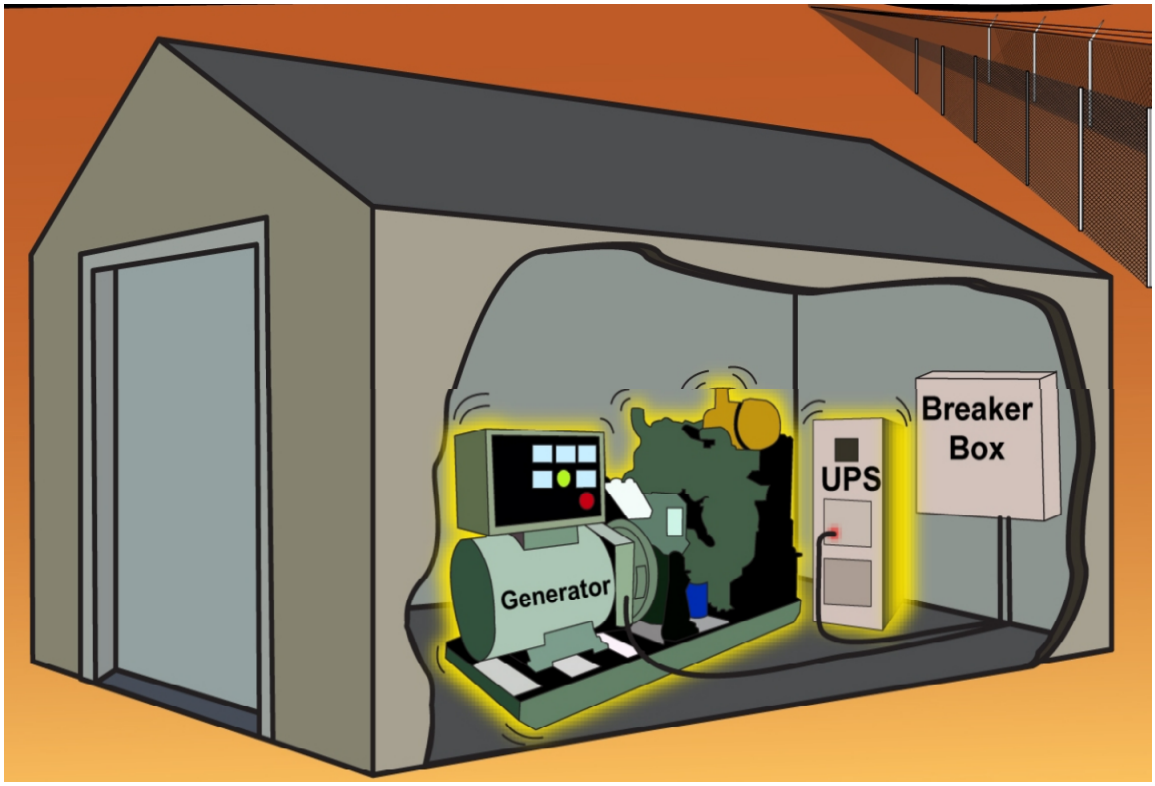

Figure 4-12 Example of a UPS in conjunction with an engine generator

In addition, the licensee should physically locate the emergency/backup power systems and their key components, including batteries, engine generators, fuel tanks, and switch gear, in an area in which they will be protected. They should either be under continual surveillance or contained in a locked enclosure with an intrusion detection system installed to protect against tampering and unauthorized access.

4.3 Alarm Assessment and Response

Assessment, which completes the detection function, is a critical component of detection and is equally important to the initiation of response. Assessment provides a means to determine the necessary actions (responses) needed to mitigate situations that pose a challenge to physical security. The key element within the assessment process is identification. Identification assists the response force in selecting appropriate responses to address security-related and potential threat situations resulting from the detected activity. Identification also provides the ability to determine the absence of a threat resulting from detected activity, such as a nuisance alarm caused by wildlife or debris. Assessment techniques must also identify the stimulus that caused the alarm quickly before the stimulus of the alarm disappears from view. This identification of the stimulus enables the initiation of timely response consistent with the goals and objectives of the physical protection program and protective strategy. Video camera coverage of each sensor zone or direct visual checks by approved personnel (e.g., individuals who meet the requirements in 10 CFR Part 37) can provide alarm assessments. However, performing alarm assessments using video is considered a best practice for assessing alarms. Unless the individual(s) performing the assessment is properly shielded and armed, direct visual assessments should primarily be used for temporary purposes, such as when the video assessment system is not functioning properly. For direct visual assessments, approved individuals (i.e., individuals who meet the requirements of 10 CFR Part 37) should be properly trained on the process/procedures for assessing an alarm. Such training should also include measures that these individuals should take in the event of an armed or violent intrusion.

4.3.1 Video Assessment

A video assessment system allows facility personnel to determine rapidly (after a sensor alarm) whether an intrusion has taken place within the facility. In addition to real-time observation of the location in which the sensor alarm occurred, the video assessment system can record and store video of alarm events and other significant event information to allow retrieval of event images within the protected area, even under conditions of multiple simultaneous alarms or delayed security personnel attention. This section provides a general overview of the video assessment systems and different components (e.g., cameras, video recording, and lighting) needed for an effective video assessment system. NUREG-1959 provides additional technical detailed information about the video assessment system and related components.

The design of the video assessment subsystem should consider the following goals:

- its ability to completely assess all sensor locations
- its ability to assess nuisance and false alarm sources
- its ability to provide system response fast enough to assess the area before the intruder leaves the area

The major components of the video assessment system include the following:

- cameras and lenses to convert an optical image of an assessed scene into an electrical signal suitable for transmission over a cable, fiber, or wireless media

- a lighting system to illuminate sensored zones evenly and to provide sufficient intensity to produce usable video images of assessed areas in low light (e.g., dark areas)

- a video transmission system that connects the cameras to the alarm station switchers and monitors

- a video switching system that takes the video from cameras and routes it to recording and monitoring display devices

- a video recording system that records video from camera feeds for archival needs or alarm event recording

- video display device (e.g., video monitors, computer, and smartphones) for displaying alarm assessment video

- an alarm communication and display controller to interface between the alarm sensor system and the video alarm assessment system to display video in the monitoring stations when a detection sensor detects activity and produces an alarm

Figure 4-13 Video assessment system

The video assessment system should be designed as a component of the total intrusion detection system. The design of the video assessment and intrusion system several should consider the following factors:

- The design should consider the layout of the intrusion sensors so that the video assessment system displays as much of the sensor zone as possible at a reasonable cost. For example, three cameras may not be necessary to cover a sensor zone; however, two cameras may be necessary for redundancy.

- The design of the video assessment system should not contribute to nuisance alarms (e.g., video or power cable noise cause sensors to alarm).

- The system should have the ability to display live video from any camera and the ability to record video from any camera.

- In addition to the automatic, integrated operation capability, the system should enable a monitoring station operator to manually control the switching of camera displays.

- The system should automatically record video before the alarm event and upon receipt of an IDS alarm and should continue to record for a short time after the alarm is received to enable video recall for further assessment.

- The system should be capable of archiving past events on a removable medium (e.g., compact disks, DVDs, or memory cards).

- Depending on the number of cameras used (e.g., more than 4), the facility or monitoring station should have at least 4 different video views—two for primary assessment video (live and recorded alarm video) and two for surveillance of video scenes generated by all cameras.

- The licensee should properly integrate common construction and installation requirements for both the intrusion sensors and video assessment systems.

4.3.1.1 Cameras

The basic function of a camera is to convert the image of a physical scene into an electrical (video) signal that is suitable for transmission to a remote display area (e.g., monitoring station). Analog or digital are the two types of communication protocols used by cameras to get the video signal to the video viewing device(s). Analog cameras produce an analog output signal in a specified format for viewing on a picture-tube-type television or flat screen digital monitor. Digital cameras or digital Internet protocol (IP) addressable cameras are generally connected to a computer network and provide a signal to the monitoring stations through the network via a stream of digital packets similar to the process that produces video on a desktop computer. Selection of an analog or digital camera and lens depends on the degree of resolution that is required. Generally, a digital camera can provide a higher resolution than an analog camera. If the facility uses a digital IP system, it may need additional security measures to protect the computer network especially if the network is linked to the facility's entire computer network. The licensee should use a separate computer network (i.e., separate security computer network) for physical protection applications.

The camera selection should also consider the following characteristics:

- High sensitivity can provide the brightest and highest contrast video image under widely varying lighting conditions.

- The camera should be able to maintain an adequate picture in the presence of bright light sources.

- The camera should be able to keep a clear picture at all points in the picture scene when motion takes place.

- The camera should have a history of reliability and durability and should be resistant to varying environmental effects.

- If the camera is digital, the output format, bandwidth, and compression should be compatible with the total video assessment system.

Resolution is the degree to which one can see fine details in a viewed image. The resolution of a video camera is generally measured using a resolution chart on which groups of equally spaced black and white lines arranged in a wedge-shaped pattern form the basis for resolution measurement. The resolution chart is marked at various intervals along the wedge patterns with the resolution values in television lines (TVLs) (analog image measurement). As a point of reference for real-time assessment, the horizontal resolution of a good quality video camera is about 600 TVLs or 800 pixels. A pixel is a digital image measurement. For assessment purposes, the licensee should consider the following three levels of resolution:

- Level of detection is the ability to detect that an object is present in the camera's field of view; however, exact identification of the object may not be possible.

- Level of classification is the ability to determine whether the object in the camera's field of view is human or nonhuman (e.g., person or animal).

- Level of identification is the ability to determine the unique identity of the human in the camera's field of view based on details of appearance (e.g., whether the intruder has a mustache and dark hair).

These three levels of resolution are dependent on camera resolution and on the size and proximity of the object in question to the camera. Therefore, the licensee should consider the possible object or target under assessment (e.g., person(s) crawling or running) when determining camera placement and the number of cameras needed. Historically, 1 percent or 6 TVLs (8 pixels) per foot of horizontal object resolution has been used as a basis for the resolution needed for intruder classification. This basis for the resolution indicates that the maximum horizontal field of view should be limited to 100 feet. Note that object resolution specification in TVL or pixels per foot should encompass all the camera-to-monitor elements (e.g., camera, lens, transmission system, video recorder, and display device) to determine the end-to-end resolution of the video assessment system.

Table 4.1 Resolution Level and Required TVLs or Pixels per Feet

RESOLUTION LEVEL	TVLs/FEET	PIXELS/FEET
Detection	1.5 to 2.25	2 to 3
Classification	4.5 to 6.75	6 to 9
Identification	7.5 to 8.25	10 to 16

Figure 4-14 Examples of classification and identification camera images

The camera imager is an important part of the camera. The imager captures the optical image and converts it to video signals. Cameras previously used tube type imagers; however, since the 1970s, cameras now use solid-state imagers. Cameras have six distinct categories: (1) black and white, (2) color, (3) day/night, (4) IR or IR enhanced, (5) intensified, and (6) thermal. Cameras with different technologies can be used together to provide a wide capability in assessment for specific applications, particularly when performing an assessment in extremely low light conditions. For example, in unlit areas, a color camera can be used during the day, and a thermal imager camera used at night.

A color camera enhances daylight scenes by providing additional color information about the target under assessment; however, nighttime use of color cameras can be problematic. When comparing color and black and white cameras with the same type of camera imager, color camera resolution is about 18 percent less than that of an equivalent black and white camera imager. The black and white camera provides a brighter, sharper, and higher-contrast image at night because of its higher resolution and operation only in the grey scale.

Day/night cameras produce color images during the day, and black and white produce images at night, thus taking advantage of the best features of both. Day/night cameras have a sensor that measures the ambient light level and controls switching from day to night mode. On some day/night cameras, the ambient light level at which the switchover occurs can be adjusted. The camera electronics monitor the output video level and switch from color to black and white when the scene illumination level is less than a predetermined level. When transitioning from day to night mode (color to black and white mode), the camera mechanically removes a near IR filter. With the camera in the black and white mode, it then responds to near IR illumination that has been blocked by a filter during the day. Removing the filter can also improve picture brightness to increase the amount of scene illumination that reaches the camera imager.

The thermal imager camera converts thermal (temperature) radiance to a video signal. Its camera video output can be a black and white image showing the temperatures of objects in shades of grey or in a gradation of colors calibrated to temperature bands. A thermal camera is a

night-vision device that responds to differences in temperatures against a background temperature reference. A thermal camera is a passive device and requires no illumination to produce a video image.

IR-enhanced cameras are low light cameras that generally operate in black and white with enhanced sensitivity to the near IR portion of the light spectrum. They require the use of a covert (hidden) IR light source to illuminate a scene. However, the IR light source can be seen if night-vision goggles are used.

Figure 4-15 IR security camera

Because cameras today are of higher quality, a good security camera system is fairly easy to find commercially. Commercially available camera systems generally include multiple cameras, a digital video recorder (DVR) with video management software, and video cables for the cameras. The licensee should consider the following items when selecting a security camera system:

- The camera(s) should have a resolution of at least 500 TVLs (i.e., classification resolution level) that covers distance of up to a 100 feet. If the camera also has night vision capability (e.g., IR illumination), most likely the viewing distance of the camera will decrease in this mode. The licensee should ensure that the night-vision mode is adequate for its application or should ensure that appropriate lighting is available to eliminate the need for the night-vision mode.

- The field of view (i.e., view angle) should be appropriate for the width of the area that the camera will be viewing. For larger areas, the licensee should use a wide-angle camera that has a greater than 60-degree view angle and should use a camera (e.g., varifocal) that has at least a 22-degree view angle for smaller areas.

The licensee should ensure that the cable length is adequate for the application. It should not purchase a longer cable without checking with the manufacturer to determine whether a longer cable will affect the camera's resolution.

- The licensee should not use a wireless camera system for video assessment because the wireless signal can be interrupted or blocked, and the camera resolution of a wireless

system is generally not as good as that of a wired camera system unless the wireless system is very expensive.

- The licensee should also purchase a camera system for smaller operations that have the ability to send a picture or video image by e-mail that can be seen on a smartphone or tablet.

- Other considerations in selecting a camera system should include a determination of how difficult it is to perform maintenance on it, the type of maintenance or warranty support that the manufacturer provides, and the presence of proper documentation to support the use of the equipment. Documentation should include operating instructions, adjustment and maintenance procedures, theory of operation, block diagrams, schematics, and replacement parts lists. Serious consideration should be given to eliminating any manufacturer's product that does not include this documentation.

Note that the video display device and video recorder that are used to display and record the alarm assessment video should have a resolution level that is equal to, or greater than, the cameras that are used (e.g., a high-definition digital camera displayed on an old cathode tube black and white television is not appropriate). In addition, if the licensee uses black and white or color cameras, it should ensure that the viewing device is able to display the same type of picture, or the detailed characteristics of the image would be hard to see. For example, the licensee should not use a black and white monitor for color camera.

Camera vulnerabilities can be created through positional errors in camera placement, mismatches in expected and actual resolution, covert tampering (i.e., by tapping into video transmission cables, inserting a recorded scene, or switching video cables to display the wrong zone), overt tampering (i.e., blinding of a camera with a bright light, covering the camera, cutting cables, or destroying the camera with a weapon), environmental conditions, and overall system response time. The licensee should take steps to remove or minimize these vulnerabilities. It should protect the video assessment system from tampering using methods, such as video loss detection, video authentication, and physical protection for cameras and cables (e.g., placing cables in conduit piping and placing cameras and video recording equipment in protective casing).

Generally, placing cameras in the corners of a room just below the ceiling provides the best assessment. The corners away from the entry points should be used to eliminate camera tampering from someone below the camera and out of the camera's field of view. The use of wide-angle lenses is best at times because these lenses provide full wall-to-wall coverage, which can eliminate or greatly minimize any blind spots within the camera field of view. In addition, tilting the camera downward helps to avoid glare from the ceiling lights, which could adversely affect the camera signal. When tall equipment is located in the area, a second camera may be necessary to observe the blind areas. A good location for a second camera may be the corner diagonally across from the first camera.

Adding cameras to a facility to help in determining the presence of a safety critical event is common practice today. For example, a camera that is used to watch products on a conveyor belt or a research experiment probably would not be properly positioned to immediately see an intruder enter a room/area. Although a facility's use of these cameras for security measures may reduce labor costs, it may decrease the effectiveness of the security system. In large or complex

facilities, separating the safety and security functions may be a better solution so that the security force will not be distracted by safety events that may mask a malevolent act. The use of these cameras may be acceptable in smaller or simple facilities; however, it may still compromise the effectiveness of a security system during an attack.

4.3.1.2 Digital Video Recording

Over the past 10 years, DVRs have almost totally replaced video cassette recorders for use in security video assessment applications and have significantly improved the process and quality of video. DVRs record video onto arrays of hard drives; therefore, they do not require the changing or rewinding of tapes. The most typical DVRs on the market today, depending on the features purchased, can do the following:

- Record the images obtained from 1 to 16 cameras simultaneously.
- Be set to record only when motion occurs in the camera scene (i.e., record prealarm and postalarm video clips for 3 to 10 seconds with about 5 seconds of optimal recording time).
- Instantaneously access recorded video from a particular time period.
- Store huge amounts of recorded video for weeks or even months.
- Adjust the number of frames per second (FPS) of video to store images from each camera, and adjust the resolution of those stored images.

Digital video image recording is a process that uses a computer to capture a video stream and to store that video information to its hard drive (or network) memory. Playing back video streams from the hard drive for operator display is then possible. The components of a digital video image recording system is generally a computer with a video recording card, video recording software for managing the storage and playback of the video images, and a display device (e.g., monitor) for displaying the video images. The video management software allows the computer to display incoming video on a monitor, record images, store incoming images to the hard drive, and play back stored images from several cameras on the monitor simultaneously.

Analog cameras separate the analog video signals into their main components (luminance and chrominance) and then convert them to a digital format for storage on a computer hard drive. Digital filters are applied to each pixel (picture element) of the video image to ensure that every single pixel of video image is represented in digital format with the highest accuracy. Once the analog video signal has been converted to a digital signal, the conversion process produces a certain amount of signal noise (white noise and other visual imperfections) that must be removed before the next step of video processing, called compression. Noise reduction software algorithms clean up the digital video information to provide better video quality, improve video encoder compression efficiency, and improve video content of the stored images.

To maximize the amount of video images that can be stored on a particular DVR system, video compression uses a coder decoder (codec) to compress video content into a reduced size format using an encoding scheme to fit efficiently onto a computer's hard drive memory. For

example, without compression, a 2-hour movie would need to be stored on 30 DVDs instead of just one DVD. Compression encoders include Motion Picture Experts Group (MPEG format), Joint Photographic Experts Group (JPEG format), Motion JPEG (M-JPEG format), and H.264 (MPEG-4). H.264 compression is currently one of the most commonly used formats for the recording, compression, and distribution of video content. Compression encoders analyze the video and decide which pieces of video information can be eliminated because they do not contain important visual content or contain redundant information, such as an image background that is all the same color.

The standard frame rate for analog cameras operating to Electronics Industry Association standards is 30 FPS. The maximum DVR video recording rate is specified in FPS. Most DVRs can record video at rates of at least 30 FPS. However, many cannot record simultaneously at that frame rate on all channels (each channel serves one camera). The maximum recording rate in FPS is divided among all the cameras served by a DVR unit, although this does not have to be an equal number of frames for each camera. If a 16-channel DVR has a maximum recording rate of 240 FPS on average and if it is recording all channels at the same frame rate, a maximum of 15 frames per channel can be allocated per channel. Because DVRs are computer based and use video management software, the Licensee can customize the number of frames that each camera can capture based on the camera, the time of day, or the type of alarm that initiates the recording.

Digital cameras can also be connected to recorders called network video recorders (NVRs) using Ethernet networks. In addition, a DVR can be implemented as a group of standalone boxes, or it can be integrated into a desktop computer-type configuration. In addition, a DVR can be used to copy video clips and images to portable memory devices (e.g., thumb drives or memory cards)
for transport from the monitoring station and for evidentiary purposes.

NVRs can also be set up to send an e-mail or text (e.g., to smartphones) with alarm video image to approved personnel and the response force for immediate response.

4.3.1.3 Lighting

Lighting for alarm assessment allows security personnel to maintain visual assessment capability during darkness or other less than optimum lighting conditions. When security lighting provisions are less than optimal, additional night-vision devices or other provisions are necessary for acceptable alarm assessment. Security lighting should be used in vital areas, such as the security zone and surrounding perimeter. Security lighting should also be used in areas in which vulnerable control points of communication, power supply, and utility infrastructure systems are located. In interior areas that conduct night operations, adequate lighting facilitates the detection of unauthorized persons approaching or attempting malicious acts within the area. Security lighting also has considerable value as a deterrent to intruders and may make the job of the adversary more difficult. Lighting is an essential element of an integrated physical protection program.

Light sources can be divided into two classes—natural and artificial. Natural lighting includes sunlight, moonlight, and stars. Artificial lighting sources include incandescent, fluorescent, mercury vapor, metal halide, and sodium vapor lights. Generally, incandescent and fluorescent

lighting are used indoors, whereas the other light sources are for outdoor applications. Incandescent lamps provide good color rendition; however, they are inefficient and have a relatively short lifetime. Fluorescent lamps provide good color rendition, high efficiency, and long life (up to 1,700 hours); however, they cannot project light over long distances. Most street lighting use mercury vapor lamps. Metal halide lighting is more efficient than mercury vapor and has better color rendition. However, mercury vapor has a longer life than metal halide (e.g., 24,000 hours versus 6,000 hours). The most efficient forms of outdoor lighting are high- and low-pressure sodium vapor lamps. However, the low-pressure lamps should not be used with color cameras because they produce an almost monochromatic yellow light. The high-pressure sodium lamps are not as efficient as the low-pressure sodium lamps; however, the high-pressure sodium lamps contain all visible frequencies, which makes them more effective when they are used with color video cameras.

Note that, when lighting is lost, varying times are required to restrike (reenergize) the light source. Restriking incandescent lamps is instantaneous, whereas restriking fluorescent lighting is almost instantaneous. Mercury vapor lamps generally take 3 to 7 minutes to reenergize, and metal halide lamps may take as long as 15 minutes. High-pressure sodium lamps take less than a minute to restrike, and low-pressure sodium lamps take 7 to 15 minutes to restrike.

The licensee should install a secure emergency power source (such as a UPS) and a power distribution system in the facility to provide power source redundancy for critical security lighting and for security detection and assessment, control, and monitoring equipment. If primary power is temporarily lost because of power system outages or hostile activity, an emergency power supply should enable critical security equipment (e.g., detection, assessment, illumination, control, and monitoring equipment) to remain operable to maintain the integrity of the physical protection system employed at the facility. Emergency power sources should be available immediately without functional interruption for critical electrical loads and should be secured against direct and indirect attack and sabotage.

An effective lighting design is of paramount importance to the proper functioning of alarm assessment systems. Just as humans need good lighting to see, most security video cameras require appropriate lighting to allow for efficient assessment of the area when natural light is not adequate or available. Optimum security lighting is achieved by adequate even light in the sensored zones. Personnel should also be able to see low contrasts, such as indistinct outlines of silhouettes, and should be able to detect an intruder who may be exposed to view for only a few seconds. Higher levels of illumination, such as that provided by deterrent lighting systems if they are properly implemented, can improve these assessment abilities.

Contrast between an intruder and the background should be an important consideration when planning for security lighting. With predominantly dark surfaces, more light is needed to produce the reflective brightness required for camera assessment than would be necessary if neutral gray backgrounds and ground cover are used. When the same amount of light falls on an object and its background, the observer must depend on the contrast of light reflected from each to determine the intruder's location. Adjusting the illumination level or the lighting location can help differentiate between background and objects of interest when contrast is poor.

Security lighting usually requires less illumination than normal task lighting except for personnel identification. Each area of a facility presents its own unique set of considerations based on physical layout, security requirements, terrain, and environmental and climatic conditions.

Information that is available from lighting equipment manufacturers and vendors of lighting analysis software to assist in designing a lighting system should include the following items:

- descriptions, characteristics, and specifications of luminaire (i.e., light fitting) and lamps
- luminaire lighting patterns
- installation layouts showing height and spacing of luminaires to achieve desired light levels
- software to produce computer-generated plots of illumination levels and lighting uniformity in a particular zone and summary statistics of the illumination profile
- average illumination level
- light to dark ratio
- maximum and minimum illumination

In planning a security lighting system, the licensee should consider the following factors:

- the cost of replacing lamps and cleaning fixtures and the cost of providing the required equipment (such as ladders and bucket trucks) to perform this maintenance
- provisions for an automatic transfer or manual override capability during a loss of primary power
- photoelectric controls for automatic control of lights during nighttime hours
- effects of local weather conditions on lighting systems for outside lighting
- fluctuating or erratic voltages in the primary power source
- grounding requirements
- provisions for rapid lamp replacement and luminaire cleaning
- special lighting requirements for critical areas (such as security zone) and for lighting that will remain operable without interruption during the loss of primary power
- continuous operation of security lighting systems during hours of darkness
- a security lighting system configuration to ensure that the failure of one or more lights will not affect the operation of the remaining lights
- restrike time (the time required before a light will function properly after a brief power interruption)
- color spectrum of bulbs

To prevent cameras from looking directly into a light source, the licensee should locate security lights above the camera and out of the camera's field of view. The security lights should generally be no less than 3 vertical meters (10 vertical feet) above the camera's position. In addition, a light source should not be positioned directly above the camera because this positioning could cause dust- or fog-induced backscatter. However, the use of a shield that extends beyond the front cover glass of a camera enclosure, like the brim of a cap, can minimize those effects. The type of lighting system used depends on the overall security requirements. Four types of lighting approaches can be used for security lighting systems: continuous, standby, movable (portable), and emergency.

Continuous lighting is the most common type of security lighting used. It consists of a series of fixed lights arranged to continuously illuminate a given area during darkness with overlapping cones of light.

Standby lighting has a layout similar to continuous lighting. However, the luminaires are not continuously lit during nighttime hours. Security personnel or the intrusion sensor system manually or automatically initiate them when suspicious activity is detected or suspected.

Movable lighting consists of manually operated, movable (portable) integrated luminaire and generator assemblies that may be operated during hours of darkness or as needed. This type of system is normally used to supplement continuous or standby lighting.

Emergency lighting is a system of lighting that may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. It depends on an alternative power source, such as installed or portable generators or battery-powered UPSs.

4.3.2 Response and Communications

Responding to an assessed alarm is the final function of the physical protection program. The regulation at 10 CFR 37.49(d) requires the licensee to request, without delay, an armed response from the LLEA to any unauthorized access involving an actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material. The NRC defines an LLEA as a public or private organization that has been approved by a Federal, State, or local government to carry firearms and make arrests and that is authorized and has the capability to provide an armed response in the jurisdiction in which the licensed category 1 or category 2 quantity of radioactive material is used, stored, or transported (i.e., 10 CFR 37.5).

The response force/LLEA could be located on site or off site. However, if the LLEA is off site, the licensee may need better detection and delay systems to account for the additional time necessary for an LLEA response. The licensee must coordinate with the LLEA, to the extent practicable, regarding how they would respond to threats against the category 1 and category 2 quantities of radioactive material (i.e., 10 CFR 37.45, "LLEA Coordination"). The licensee must provide the LLEA with descriptions of the facilities, the risk-significant radioactive material, and its established security measures for protecting the risk-significant radioactive material (i.e., 10 CFR 37.45).

The licensee should schedule joint training exercises periodically with the response force and any other internal or external organization (e.g., facility management, corporate management, the local fire department, the nearest hospital, the Federal Bureau of Investigation, the NRC, and Agreement State regulators) that may play a part in responding to a threat at the facility. This training should include the following discussions:

- the facility layout
- different roles that each organization may fill or provide in the event of a threat
- communication procedures (i.e., who is called, and when is the call made?)
- descriptions of the category 1 and category 2 quantities of radioactive material, the potential hazards if an individual(s) is exposed to it, and the potential harm it could cause if it is stolen or sabotaged
- actions that need to be taken if an adversary is successful

Additionally, the licensee should provide updates to the LLEA if information about the facility, the risk-significant radioactive material, or the storage and use of the radioactive material changes.

Caution should be taken in regard to the level of information that is provided during these exercises. Depending on who is attending the training and on the location of the exercise, sensitive security-related information should not be discussed (e.g., intrusion sensor type and location, combinations to doors, and types of weapons that will be used in case of a threat). Generally, a mock scenario (i.e., tabletop or actual real-time scenario) is the best way to approach the training exercise.

Communication is a very important part of the response function. The licensee needs to transmit information about an adversary's actions to the response force quickly and reliably. The alarm monitoring station generally contacts the response force (i.e., the LLEA). The type of communication used to contact the response force generally depends on whether the response force is located on site or off site. If the response force is located off site, the licensee would generally contact them by telephone (e.g., landline or cell phone). Note that, if the licensee and the LLEA use cellular phones to communicate, the adversary could have equipment that could intercept/disrupt the cell phone signal. Therefore, the licensee should preferably use a landline to communicate with the response force and should use a cell phone as a secondary method of communication.

If the response force is located on site (i.e., at the facility), the licensee would generally contact it by an internal communication system (e.g., intercom system), a radio system (e.g., battery-operated handheld radio), or telephone.

If the licensee uses a conventional radio system, it should assume that adversaries are eavesdropping on the transmission. Therefore, security personnel must determine what information to release on the radio. Radio communications should be limited to only those transmissions that are absolutely necessary and that cannot be communicated by more secure methods, such as landline telephones and intercom systems. Once the adversary obtains the

radio frequency being used, he or she can transmit deceptive messages as an attempt to confuse members of the response force. Voice-private radios can help make a radio network resistant to eavesdropping because it can scramble or digitally encrypt the messages. In addition, to help protect against deceptive messages, the licensee should use authentication codes to verify that the transmission was made by a member of the response force and not by an adversary.

To maximize the security and reliability of the radio network, the licensee should develop procedures, should perform personnel training and equipment maintenance, and should ensure that an alternate means of communication is immediately available. Procedures should include instructions on how to use the radio (e.g., how to operate the radio and the use of authentication codes) and periodic maintenance requirements (e.g., testing and changing batteries). An alternate means of communication should always be available in case primary communications fail, are interrupted (e.g., jammed), or are compromised (e.g., eavesdropping). A procedure for simply switching to an alternate radio channel could provide a second means for communication. However, the licensee should ensure the availability of different types of communication devices, such as a telephone (e.g., landline or cell phone), an intercom system, or pagers, or communication methods, such as transmitting messages by hand signals, lights, or whistles.

5. PHYSICAL SECURITY BEST PRACTICES FOR MOBILE AND TRANSPORTATION OPERATIONS

This chapter describes the protective measures and best practices that licensees should use for mobile devices that contain risk-significant radioactive material (e.g., radiography cameras and well logging devices) and for the transportation of risk-significant radioactive material. The mobile use and transportation of risk-significant radioactive material is particularly vulnerable to malicious acts, such as theft or diversion. Therefore, it is important that adequate delay, detection, tracking, and communication mechanisms are in place to provide time for a local law enforcement agency (LLEA) to interrupt or neutralize the adversary before the malicious act occurs or to provide immediate notification of the theft and initiate recovery actions. A defense-in-depth strategy is a key component in an effective physical protection program for mobile and transportation operations.

A defense-in-depth strategy uses multiple layers of protective measures that an adversary has to overcome to accomplish his or her goal. The existence of these layers will require an adversary to avoid or defeat a number of different protective measures in sequence to succeed. For example, an adversary might need to penetrate two or more separate barriers (e.g., a vehicle disabling system and high-security locks) before he or she can remove a mobile device that contains risk-significant radioactive material. A defense-in-depth strategy generally serves as a deterrent for an adversary because it adds uncertainty and, therefore, requires the use of different techniques and tools and creates additional steps. This type of strategy also adds to the overall reliability of the protective measures because it eliminates dependency on one protective measure, creates vital redundancy, and protects against a single point of failure.

5.1 Vehicle/Trailer Alarm and Disabling Systems

The licensee should use a vehicle or trailer alarm system to detect an intruder when carrying risk-significant radioactive material. The vehicle or trailer alarm system should have the ability to detect unauthorized entry into any access or open point in the vehicle or trailer that leads to the risk-significant radioactive material or to the ignition of the vehicle. Many different types of alarms and alarm systems can be used on a vehicle or trailer. The licensee should consider the following types of vehicle alarms/sensors for the alarm system based on the type of vehicle (e.g., a car, pickup truck, or tractor trailer) or trailer that it uses to carry risk-significant radioactive material:

- a door sensor alarm that will automatically go off if the door, hood, or trunk/cargo door is opened
- a window sensor alarm that will go off if the window is shattered
- a shock sensor alarm that will set off the vehicle alarm if the vehicle is moved
- a pressure alarm that will go off if the internal air pressure changes due to the opening of a door or window
- a tilt sensor alarm that will go off if the intruder tries to raise (e.g., tow) the vehicle or trailer

Some other features that the licensee should consider for the vehicle or trailer alarm system are ability to disable the ignition when an alarm is triggered and the ability to contact an entity that is not transporting the risk-significant radioactive material, such as an approved individual, the licensee, or the LLEA by sending a message to a pager, cell phone (e.g., smartphone), or an alarm-monitoring call center (e.g., movement control center). Note that the range for sending a message out can vary depending on the alarm system. The licensee should ensure that the alarm systems ability to communicate is appropriate for the specific operations.

For devices that contain risk-significant radioactive material that are located in or on a vehicle or trailer, the licensee must use a method to disable the vehicle or trailer when it is not under direct control and constant surveillance by the licensee (10 CFR 37.53(b)) unless the health and safety requirements for a site prohibit the disabling of the vehicle. The objective of the vehicle-disabling requirement is to delay unauthorized removal of a device or radioactive material by stealing the vehicle on which it is secured. Examples of acceptable vehicle-disabling methods would include trailer hitch locks, wheel locks (boots), or methods to disable the vehicle's engine. The licensee cannot consider the removal of a key from the ignition of a vehicle sufficient for disabling its engine because an adversary can start it without using the key (e.g., use of a duplicated key or hot-wiring techniques).

5.2 Vehicle/Trailer and Package Tracking Systems

For risk-significant radioactive material that is being transported, the ability to track the location of the vehicle, trailer, or package that contains risk-significant radioactive material is very important. Tracking of the material is also an NRC requirement (10 CFR 37.79(a)(1)(iii) and 10 CFR 37.79(a)(3)(i)). Several different methods can be used to track a vehicle, trailer, or package. One of the more common ways to track a vehicle, trailer, or package is by using a global positioning system (GPS). A GPS is a space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near Earth that has an unobstructed line of sight to multiple GPS satellites. GPS tracking devices are commercially available, and they can also be found already installed in some vehicles (e.g., newer General Motor vehicles have the OnStar GPS System). A GPS tracking device (receiver), which is located on the vehicle, trailer, or package, works by receiving and sometimes sending a signal to a satellite. Computer software tracks the location of the GPS device.

GPS tracking devices are typically classified as active or passive devices. A passive device stores information, such as GPS location, speed, and heading, and once the vehicle returns to a predetermined point, the GPS device is removed, and the data can be downloaded to a computer for evaluation. Some passive systems are automatic download types that transfer data via wireless download. Active GPS devices collect the same information but generally transmit the data in near real time via cellular or satellite networks to a computer or data center for evaluation. The licensee should use only active GPS tracking devices when transporting risk-significant radioactive material. Mounting the GPS device on the vehicle, trailer, or package container is also considered a best practice. In addition, an adversary should not be able to easily detect the location of the GPS device.

Some GPS tracking systems can implement an "electronic fence" along the course of the approved route to or from the jobsite or delivery location and can provide notification of any diversions off this route. However, licensees should be cautioned that, if the system is only

tracking the vehicle and not the vehicle contents (e.g., a package that contains risk-significant radioactive material), precious time could be spent tracking a diverted truck in one direction while the adversary has the radioactive material that is no longer being tracked. For this reason, the licensee should be constantly aware of the vehicle and package movement and should have reliable and frequent communications with the individual(s) transporting the material.

Another common practice for tracking a package is to use carriers (e.g., U.S. Postal Service and FedEx). Carriers use various methods, such as GPS, radio, or wireless communication, to track packages. For packages that contain risk-significant radioactive materials, the licensee should ensure that the carrier has an established package tracking system that is documented, proven, and reliable and that is routinely used to transport objects of value. For a package tracking system to maintain constant control or surveillance, or both, it must allow the shipper or transporter to identify when and where the package was last and when it should arrive at the next point of control (i.e., 10 CFR 37.79(a)(3)(i)).

5.3 Locks and Locking Systems

Locks and locking systems are also important elements for securing the vehicle or mobile device, or both, containing risk-significant radioactive material. Although some locks are difficult to pick or manipulate, no lock can claim to be "manipulation proof." Therefore, the licensee should use locks in conjunction with other security measures, such as a vehicle alarm system. In all applications, the goal should be to make the lock delay time and capability closely match the penetration resistance of the rest of the secured barrier (e.g., vehicle or container).

When securing a mobile device, vehicle, or trailer that contains risk-significant radioactive material, the licensee should only use only high-security locks or locking systems that are made to secure high value items. Shrouded locks, multiple-point locks, puck locks, and shackle locks are examples of high-security locks. In addition, the licensee should use chains or wires made for high-security applications to secure containers or devices that contain risk-significant radioactive material. An example of a high-security chain or wire cable is a chain that has a diameter of at least 13 millimeters (0.512 inches) of hardened steel or a twisted steel wire cable that has a thickness greater than 6.35 millimeters (0.25 inches).

Figure 5-1 Puck lock and shield used on a cargo van

5.4 Communications and Response

When transporting risk-significant radioactive material, the ability to effectively communicate with outside entities, such as a movement control center, escorts, and the LLEA, is very important. To determine what should be considered a loss of communication, the licensee should identify foreseeable normal and contingency scenarios and should consider their likely urgency in deciding how many times the communications center, driver, or escort should try to restore the primary means of communication before resorting to the secondary means. For example, in an accident or a security emergency, the communicator should not delay in resorting to the secondary means of communication. The protocol should also allow the communicator to take into account the severity of static and the urgency of a situation in determining the extent to which the degradations of communication clarity justify switching to the alternate communication technology. Redundant or secondary communications should also mitigate an interruption caused by either natural events, such as storms, or deliberate actions, such as signal jamming, that may cause a loss of communications on the primary communication device. One or more additional communication devices should be available to operate independently from the primary device, thereby minimizing the possibility that whatever disabled the primary device will also affect the redundant devices.

Communication protocols should include a strategy for the use of authentication codes and duress codes and provisions for refueling or other stops, detours, and locations at which communication could be temporarily lost. An acceptable protocol may use a number of methods and technologies or combinations of them for duress and authentication codes. The primary purpose of an authentication code is to enable a licensee to confirm that the radioactive material remains in the physical possession of an authorized employee of the licensee or carrier. The purpose of a duress code is to enable a licensee to confirm that the individual at the offsite location who initiated the communication or who is responding to the licensee's call is not being forced to provide false information.

For example, to frustrate any attempt by an unauthorized individual to delay an investigation or to call off an ongoing recovery effort prematurely, the licensee should be able to confirm through its pre-established authentication protocol the true identity of the employee, regulatory agency representative, or law enforcement officer reporting from an offsite location. The licensee can accomplish authentication by using an agreed upon separate radio frequency or alternative communication method, asking the caller to appear before a video camera on the vehicle to display a photo identification badge, asking for the correct answer to one or more agreed upon questions, or using a combination of these methods.

Questions should require specific responses that are of a personally distinguishing nature (e.g., the name of a first pet) or that otherwise are not so intuitively obvious that an adversary could infer the correct response. Similarly, the licensee or carrier may use one or several of these techniques in combination in a pre-established protocol or code word or phrase to signal that the driver or accompanying individual is under duress (e.g., at gunpoint or within lethal range of an explosive.) The duress code should permit the driver or accompanying individual to introduce the code on his or her own initiative without prompting, and it may involve seemingly mission-related technical questions and answers, apparently offhand remarks, or some other conversational technique. The duress code should enable the offsite individual to signal without arousing suspicion that he or she is making a false report under threat by an adversary who is not visible or who is obviously malevolent to the licensee or call center personnel.

Along with knowing all of the communication protocols, the licensee and the individuals transporting the risk-significant radioactive material should know any specific procedures for requesting a response. The licensee should provide information to the driver or the approved individual transporting the radioactive material that indicates the LLEA contact information (e.g., phone number and physical address). If different LLEAs are located throughout the scheduled route, the licensee should provide a map or some type of identifying information that indicates the appropriate LLEA that the driver or the approved individual should contact at specific areas along or near the scheduled route.

When transporting category 1 quantities of radioactive material, licensees are required to identify "safe havens" along the schedule route. A safe haven is defined as a readily recognizable and readily accessible site at which security is present or from which the transport crew can notify the LLEAs in the event of an emergency and wait for them. The licensee should use the following criteria to identify safe havens for shipments:

- The safe haven is near the route (i.e., readily available to the transport vehicle).
- Security from Federal, State, or local assets is present or is accessible for a timely response.
- The site is well lit, has adequate parking, and can be used for emergency repair or for waiting for the LLEA response on a 24-hour basis.
- Additional telephone facilities are available if the communications system of the transport vehicle fails to function properly.
- Possible safe haven sites include Federal sites that have significant security assets, such as gates on military bases or guarded agency parking lots; secure company terminals; State weigh stations; State welcome stations or rest areas; scenic overlooks or visitor centers; truck stops with secure areas; and LLEA sites, including State police barracks.

Even though the NRC requires a licensee to identify safe havens when transporting category 1 quantities of radioactive material, it should, as a best practice, identify safe havens when transporting category 2 quantities of radioactive material.

6. REFERENCES

1. Regulatory Guide 5.12, “General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials,” U.S. Nuclear Regulatory Commission, Washington, DC, November 1973.

2. MIL-HDBK-1013/1A, “Military Handbook: Design Guidelines for Physical Security of Facilities,” U.S. Department of Defense, Washington, DC, December 15, 1993.

3. Garcia, M.L., *The Design and Evaluation of Physical Protection Systems*, Second Edition, Butterworth-Heinemann, Burlington, MA, 2008.

4. International Atomic Energy Agency (IAEA) Nuclear Security Series No. 11, “Security of Radioactive Sources,” International Atomic Energy Agency, Vienna, Austria, May 2009.

5. Regulatory Issue Summary 2010-02, “The Global Threat Reduction Initiative (GTRI) Federally Funded Voluntary Security Enhancements for High-Risk Radiological Material,” U.S. Nuclear Regulatory Commission, Washington, DC, January 21, 2010.

6. Radiation Source Protection and Security Task Force report entitled, “The 2010 Radiation Source Protection and Security Task Force Report,” U.S. Nuclear Regulatory Commission, Washington, DC, August 11, 2010.

7. World Institute for Nuclear Security (WINS) report entitled, “A WINS International Best Practice Guide: Security of Well Logging Radioactive Sources,” Revision 1.0, World Institute for Nuclear Security, Vienna, Austria, December 2010.

8. IAEA Nuclear Security Series No. 13, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities,” INFCIRC/225/Revision 5, International Atomic Energy Agency, Vienna, Austria, January 2011.

9. NUREG-1959, “Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees,” U.S. Nuclear Regulatory Commission, Washington, DC, March 2011.

10. NUREG-1964, “Access Control Systems: Technical Information for NRC Licensees,” U.S. Nuclear Regulatory Commission, Washington, DC, April 2011.

11. NUREG-2155, “Implementation Guide for 10 CFR Part 37, ‘Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material,’” U.S. Nuclear Regulatory Commission, Washington, DC, February 2013.

12. Title 10 of the *Code of Federal Regulations* (10 CFR) Part 37, “Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material,” U.S. Nuclear Regulatory Commission, Washington, DC, March 2013.

APPENDIX A

DEVELOPING A PHYSICAL SECURITY PLAN

Licensees that possess an aggregated category 1 or category 2 quantity of radioactive material must develop a written security plan that is specific to their facilities and operations and that meets the requirements in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material." The purpose of the security plan is to establish the overall security strategy to ensure the integrated and effective functioning of the security program. To comply with 10 CFR Part 37, the security plan must, at a minimum, describe the measures used to implement the physical protection program and to identify the security resources, equipment, and technology needed to effectively implement the physical protection program.

The specific measures that licensees must implement under the security program include, among other things, the establishment of security zones; the design and procurement of a physical protection system for monitoring, detection, assessment, and alarm/communications; the procurement of any necessary support services, such as commercial security services; and coordination with local law enforcement agencies (LLEAs). The program must also include recordkeeping measures and must provide for the operation, testing, and maintenance of equipment and technologies that, when they function as an integrated system, are designed to effectively monitor and, without delay, detect, assess, and respond to an actual or attempted unauthorized access to category 1 or category 2 quantities of radioactive material. (See 10 CFR Part 37 for specific requirements.) The suggested template below includes information that the licensee should consider in its security plan.

SECURITY PLAN CONTENTS

MEASURES AND STRATEGIES

1. Introduction
   - 1.1 Plan Requirements
   - 1.2 Objective of the Security Plan
   - 1.3 Scope
   - 1.4 Periodic Review and Update of the Security Plan
   - 1.5 Retention of the Security Plan
2. The Facility
   - 2.1 Overview
   - 2.2 Risk-Significant Radioactive Materials
   - 2.3 Categorization of Radioactive Materials
   - 2.4 Physical Description
   - 2.5 Operational Description
   - 2.6 Regulatory Requirements
3. Security Management
   - 3.1 Roles and Responsibilities
   - 3.2 Training and Qualifications
   - 3.3 Access Authorization
   - 3.4 Trustworthiness and Reliability
   - 3.5 Performance Testing
   - 3.6 Maintenance
   - 3.7 Budget and Resource Planning
   - 3.8 Information Protection

RESOURCES, EQUIPMENT, AND TECHNOLOGY

4. Security System
   - 4.1 Security Assessment Methodology
   - 4.2 Security System Design
   - 4.3 Access Control Measures
   - 4.4 Delay, Detection, and Assessment Measures
5. Security Procedures
   - 5.1 Routine, Off-Shift, and Emergency Operations
   - 5.2 Opening and Closing of the Facility
   - 5.3 Key and Lock Control
   - 5.4 Radioactive Source Inventory and Accounting
6. Response
   - 6.1 Response Plan and Arrangements
   - 6.2 Communications
   - 6.3 Emergency Response and Contingency Planning
   - 6.4 Increased Threat Level
   - 6.5 Security Event Reporting

References

Appendices

MEASURES AND STRATEGIES

1. INTRODUCTION

This section should describe why the security plan is required and what objectives it satisfies and should include any scope considerations.

1.1 Plan Requirements

The section should describe the need for the security plan under the particular circumstances of the facility, such as to (1) satisfy the need to adequately protect risk-significant radioactive materials against a threat of unauthorized removal or sabotage, (2) satisfy regulatory requirements, and (3) be a part of, and be integrated with, the organization's operational management system.

1.2 Objective of the Security Plan

This section should describe the objectives that the security plan will satisfy, such as to (1) document the design and operation of the security system and security management measures according to applicable methods, criteria, and requirements, (2) demonstrate regulatory compliance by specifying, in each relevant section, which particular regulatory requirement is met, and (3) serve as an operational tool that is used by management and staff and that will be regularly updated and improved.

1.3 Scope

This section should describe the coverage and any limitations of the security plan and its relation to other relevant documents or arrangements, such as any management, operational, radiation protection, or emergency matters.

1.4 Periodic Review and Update of the Security Plan

This section should describe the document's status, such as its preparation, the individual who will review and approve the plan (i.e., the individual with overall responsibility for the security program under 10 CFR 37.43(a)(3)(i)), and related document control matters. (Note that these elements may be evident as part of the document's format if they are within the organization's document control or quality management system). This section should also describe examples of conditions that may require the licensee to revise its security plan (e.g., new threat information, changes in facility operations, or any other development that could affect the performance of the security system). It also explains how the licensee will review and update this security plan. For example, what will the review entail, and when will the licensee perform the review (a specific time interval, such as annually)? In addition, this section will explain how the licensee will instruct affected individuals on any revisions to the security plan before implementing them, particularly those individuals whose responsibilities or job duties are affected by such revisions.

1.5 Retention of the Security Plan

This section will describe how the licensee will maintain the security plan. It will describe the record retention period of the security plan. Security plans must be retained for 3 years after the plan is no longer required. If any portion of the security plan is superseded, the previous version shall be maintained for 3 years after the record is superseded (i.e., 10 CFR 37.43(a)(4)).

2. THE FACILITY

This section should describe the materials and locations that need protection, the level of protection, and the physical and operational environment that affects such protection.

2.1 Overview

This section should describe the purpose or mission of the facility and its operating organization, including the types of practices involving nuclear and radiological materials and their associated devices or equipment.

2.2 Risk-Significant Radioactive Materials

This section should provide details of the risk-significant radioactive materials and their associated equipment, such as isotope, activity and reference date, chemical and physical form, serial number, equipment and device brand, model, and manufacturer.

2.3 Categorization of Radioactive Materials

This section should identify and explain the basis for the categorization of the radioactive materials, including aggregated material (e.g., contains category 1 or category 2 quantities of radioactive material with a total activity or range of activity that exceeds the category 1 or category 2 thresholds defined in Appendix A, “Category 1 and Category 2 Radioactive Materials,” to 10 CFR Part 37).

2.4 Physical Description

This section should describe the physical aspects of the facility and its surrounding environment, including diagrams and scale floor and building drawings and photographs. These physical aspects should include the following information:

- location and layout of the facility that particularly indicate areas accessible to the public, roads, and parking areas; the nearest public thoroughfares; the central security office, if applicable; the building and site perimeter, access points, and physical barriers

- the site’s surrounding environment, such as industrial, commercial, residential, or other uses; an indication of distances to the nearest LLEA and other services; its proximity to other buildings, roads, and other features of security or operational interest

2.5 Operational Description

This section should describe the facility operations, including working and nonworking hours; the number and type of staff involved in the facility's operation; the typical number and type of other people, such as visitors, members of the public, patients, customers, service personnel, and contractors, who may be at the facility according to scheduled operations or at any other time.

2.6 Regulatory Requirements

This section should identify and reference the regulatory requirements pertinent to security due to the type of practice or facility, the risk-significant radioactive material(s), and any other relevant requirements. Note that the licensee could reference the particular regulatory requirement in other relevant sections of the security plan by stating the applicable provision of the regulations, license, standards, or other requirement.

3. SECURITY MANAGEMENT

This section should describe the security management or security organization measures in place and the particular duties of management and staff in ensuring that the security measures are implemented and effective.

3.1 Roles and Responsibilities

This section should identify the positions required for the facility's operations and should describe the roles and responsibilities of those positions, including management, supervisor, staff, and contract personnel positions; positions directly responsible for facility security; and positions with responsibility for regulatory matters, such as the Radiation Safety Officer.

The licensee should consider using an organizational chart, a schematic, or tables showing the staffing structure with lines of authority and supervision.

3.2 Training and Qualifications

Using the information on positions with security responsibility from Section 3.1, the section should include the following descriptions:

- qualifications for employment, including any specific qualifications required by regulations or license conditions

- training that the organization or facility will provide to each individual with security responsibilities, including the required initial, specialized, or advanced training for the position and any other relevant specific on-the-job or refresher training, such as training that involves procedures and work instructions

- the provider and frequency of the training

- related training records that document satisfactory completion of initial and refresher training

3.3 Access Authorization

This section should describe the process necessary for authorizing personnel who need unescorted access to the risk-significant radioactive material location or secured areas, or both, and access to security-sensitive information to perform their duties (which may or may not be directly related to security). The description should ensure that the process does the following:

- Identifies the positions that require unescorted access.
- Verifies that the individuals who hold the positions are trustworthy and reliable (Section 3.4).
- Verifies that the individuals who hold the positions have the necessary qualifications and training (Section 3.2).
- Maintains up-to-date records of personnel approved for unescorted access.
- Withdraws access authorization when personnel no longer have a need for unescorted access, such as transfer of job responsibilities or termination of employment.

3.4 Trustworthiness and Reliability

This section should describe the process for evaluating the trustworthiness and reliability of personnel to determine whether they should be granted unescorted access to nuclear and radiological materials, secured areas, or security-sensitive information. The management process or procedure for evaluating the trustworthiness and reliability of personnel should also indicate requirements for periodic review and any reevaluation for particular circumstances. The description should clearly do the following:

- Identify the individuals or job descriptions whose trustworthiness must be evaluated
- Identify the applicable requirements regarding trustworthiness and reliability in regulations for the security of risk-significant radioactive materials, license conditions, or elsewhere, including any requirements that vary depending on other factors.
- State what records must be maintained and kept confidential as part of the trustworthiness and reliability evaluation.

3.5 Performance Testing

This section should describe the facility's performance testing process for verifying the effectiveness of security equipment, systems, and personnel, such as access control systems, intrusion detection sensors, alarm assessment, alarm station operations, and alarm response. The description of the process should include the records generated, the schedule and arrangements to record, and action deficiencies.

For each performance test, this section should describe critical information about the test, including the following:

- performance test objectives stating what is to be accomplished by conducting the test
- references to the manufacturer's/supplier's document or operating procedure that establishes the performance requirement
- performance test procedures and conditions for conducting the test
- criteria for evaluating the results of the test
- performance test control measures taken to ensure that the test is valid and will not result in injury to personnel
- resources or equipment, or both, that are needed to conduct the test
- coordination requirements, such as who must approve or acknowledge the conduct of the test

In addition, the licensee should consider identifying those barriers and any other security system elements that cannot be adequately tested and should explain how the absence of performance tests for those elements will not compromise the facility's protection.

3.6 Maintenance

This section should describe the maintenance program for the facility's security systems (i.e., intrusion detection systems, associated communication systems, and physical components of the security system) to ensure their continuous and reliable operation and should include the following information:

- The section should describe the approach used to conduct preventive and corrective maintenance. This approach can be based on one of three options. In the first option, the facility management contracts with an outside security vendor to maintain the equipment. The second option involves using facility technicians who are qualified to maintain the security equipment. The third option involves using a combination of qualified facility technicians to perform preventive maintenance and outside security vendors to perform corrective maintenance as required. The licensee should choose the specific maintenance approach based on which option is most practical and cost effective for the facility. Factors, such as total maintenance program cost, nature of facility operations, and resources available, will influence the licensee's choice of maintenance approach.
- The section should include the roles and responsibilities of contractors and facility staff. (Note that these will be determined by the maintenance approach.) It should specify the roles and responsibilities of facility staff in the maintenance of security equipment. The description of roles and responsibilities should state who has overall responsibility for maintenance and who has the authority to conduct each particular type of maintenance.

- If a contractor is employed for the maintenance of security equipment, the description should identify the contract and those major tasks that the contractor is required to perform. If the licensee chooses a hybrid maintenance approach, this section should describe explicitly who does what.

- The section should include a master equipment and spare parts list with warranty information. In addition, it should describe those critical subsystems or components that, in the event of failure, would require a long time to procure and would therefore create a vulnerability. Factors, such as cost, procurement lead time, and security system vulnerability, should determine the definition of criticality of subsystems or components.

- The section should include a schedule of preventive maintenance activities for each subsystem or component. Modern security equipment requires periodic routine preventive maintenance to ensure reliable operation. Standard industry practice for the frequency of routine preventive maintenance is every 3 months. More sophisticated systems that incorporate biometric sensors or other special detection means may require more frequent attention.

- The section should include arrangements for dealing with component failures, including corrective maintenance response time and identification of compensatory measures required during inoperability. This section should describe the actions that will be taken when a subsystem or component fails during normal operation or during testing. The description should include notification procedures and contractor response time as specified in the applicable contract. The description should also outline compensatory measures, such as the employment of additional security personnel or the modification of operational procedures, or both, to offset the loss of a technical security measure.

- The section should identify maintenance records and documents that the licensee must maintain to verify the existence of an ongoing maintenance program for security equipment. It should specify the length of time the maintenance and testing records must be retained. At a minimum the licensee should retain the following records:

  – routine preventive maintenance

  – corrective maintenance actions

  – equipment warranty records

  – equipment replacement

  – results of operational testing

- The section should identify trends, such as nuisance alarm rates, false alarm rates, and alarm failures.

- The section should include equipment replacement planning. Most modern security system components have a 5- to 7-year life cycle.

This section should also describe the process for routinely evaluating the security system and for projecting the retirement and replacement of security system components or the entire system. This information will inform the security program budget and resource planning.

At a minimum, this section should identify the following information on equipment:

- the date when the equipment was placed into service
- the cost for the procurement and installation of the equipment, which should be identified at the subsystem and component level
- the anticipated effective life of the equipment at the subsystem and component level
- anticipated annual inflation

3.7 Budget and Resource Planning

Resource planning for security should be viewed and implemented at the system level. This section should describe the requirements to establish a budget for all activities and associated elements that affect security. At a minimum, these requirements should include the following items:

- human resources
- training
- technical means of security (i.e., incorporating information from the maintenance requirements in Section 3.6)
- equipment maintenance
- all other activities associated with security management

3.8 Information Protection

If applicable, this section should describe the digital computers, digital communication systems, and digital networks used for the security system or the risk-significant radioactive material safety-related systems, or both, and should explain how these digital systems will be protected. Based on the potential for certain information to compromise security if it is disclosed to unauthorized persons, this section should include the following information:

- a description of the information that requires protection, as defined by the regulatory body or facility management requirements, including the following items:
  - the location and inventory of sources/material
  - the security system design, equipment details, and diagrams
  - lock combinations and key codes

  - threat and vulnerability assessment information
  - planned dates, routes, and mode of shipment or transfer of sources/material
  - security plans and procedures, contingency plans, response plans, and related arrangements and measures

- an explanation of how the licensee identifies the protected information, such as the use of markings or other designators that will ensure that all users of this information recognize it as requiring protection
- description of the particular forms of the protected information, such as paper documents, electronic media, and security video recordings
- information about where the protected information is stored and who has custody of this information
- identification of who has access to this information and an explanation of how the licensee determines access (e.g., based on job requirements and the appropriate level of trustworthiness and reliability (Sections 3.3 and 3.4)
- discussion of the protection measures that the licensee has established to prevent unauthorized access during use or storage of the information (e.g., physical protection and encryption)
- a description of the requirements that the licensee has established to prevent unauthorized access during the reproduction and transmittal of protected information within or outside the facility
- an explanation of how the licensee destroys protected information to prevent its recovery when it is no longer needed, including identifying the individual(s) who is authorized to destroy such information and describing the means by which the various forms of information are destroyed

RESOURCES, EQUIPMENT, AND TECHNOLOGY

4. SECURITY SYSTEM

This section should describe how the current security system is designed and implemented. It should follow the standard practice of identifying the specific target(s) (radioactive source(s)) under protection, identifying and assessing the threats against which the facility is being protected, describing the security assessment methodology, and providing information on how the design of the security system achieves sufficient protection by using a graded approach and by employing the principles of defense in depth and balanced protection.

4.1 Security Assessment Methodology

This section should describe the process or methodology used to evaluate the security system of the facility and assess its vulnerabilities. The description should indicate the results of the initial security assessment as input to the security system design (Section 4.3), the periodic updates as part of the security plan review and licensing requirements (Section 1.4), changes necessary to address new threat information, changes in facility operations, or any other development that could affect security system performance or vulnerabilities.

4.2 Security System Design

This section should describe how the security system has been designed and integrated at the facility level to provide the level of protection required, taking into account the graded approach and the principles of defense in depth and balanced protection. It should describe the security layers and should explain how each secured area and associated radioactive source is protected by detection, delay, and response measures in an integrated and balanced way, particularly indicating the design and function of the structural, technical, personnel, and organizational measures. This description should identify the type of equipment and systems installed and their locations.

4.3 Access Control Measures

This section should describe the physical measures for controlling access and should include the following factors:

- an explanation as to how personnel are physically controlled at each access control point to limit access only to approved individuals according to the access authorization procedure (Section 3.3) and to prevent unauthorized access

- the specific means used to authenticate the identity of approved individuals, such as key cards, PINs, a biometric device, or a combination of all these methods

- the procedures to be followed by approved individuals to access a secured area

4.4 Delay, Detection, and Assessment Measures

For each of the controlled or secured areas, this section should describe the following items:

- barriers (delay measures) used to increase adversary task time relative to response time, including high-security-hardened metal doors, high-security locks, and reinforced grids on large openings or windows into the controlled or secured areas, such as buildings, topography, fences, walls, and doors

- means of detection at each barrier, including, as applicable, both intrusion detection systems and observation by facility personnel

- method of assessment, including the people and equipment supporting the assessment, such as video camera monitoring and switching systems, central alarm stations, internal and external guard or response forces, computer and recording systems, security lighting, electrical and backup power sources, and communications measures

5. SECURITY PROCEDURES

This section should describe the written procedures that provide instructions to the responsible personnel for operating and maintaining the security measures. The actual procedures should be written as standalone documents that an appendix to the security plan could include.

5.1 Routine, Off-Shift, and Emergency Operations

This section should describe how assigned personnel, such as staff and contractors (e.g., cleaners and maintenance), will operate security systems and will discharge their other security-related responsibilities during periods of routine operations; off-shift or after-hour operations when staff are not ordinarily present (generally at nights, on weekends, and during holidays); and emergency operations when a security-related or other emergency occurs, such as an unauthorized entry into a secured area.

5.2 Opening and Closing of the Facility

This section should describe the procedures for opening and closing each secured area within the facility, particularly activities, such as the unlocking and locking of doors and other barriers, and communications with the alarm station to activate and deactivate detection systems. The procedures should identify the individual(s) within the organization responsible for opening and closing these areas and should also include actions to validate that other delay mechanisms (e.g., cages) have been appropriately secured.

5.3 Key and Lock Control

The section should describe the procedures used to control all keys, locks, combinations, access/alarm codes or passwords, and related devices used to control access to secured areas and security systems. The procedures should identify the individual(s) responsible for changing these access control devices and the specific conditions under which the devices must be changed, such as the compromise of a combination or access/alarm code or password, the loss of a security key, or the removal of access authorization for personnel.

5.4 Radioactive Source Inventory and Accounting

This section should describe how the licensee performs periodic accounting for each radioactive source (as prescribed by the regulatory body) and should include the following information:

- the accounting method used, such as a physical check, remote video monitoring, examination of seals or other tamper-indicating devices, or radiation measurements

- records generated that indicate the results of each verification, including information about when the verification was done, who performed it, and what method was used

- arrangements for corrective actions and reporting if the presence of a radioactive source cannot be verified

The section should also describe how the facility established and currently maintains an inventory of risk-significant radioactive material, including information required by Security Plan Item No. 2.2 above; radioactive source use history, including its movement into, within, and out of the facility; the receipt, transfer, or disposal of the source; and other information, as appropriate, to enable the source to be identifiable and traceable.

6. RESPONSE

The licensee should conduct response planning, tabletop exercises, and response exercises jointly with any external organizations involved in responding to a security incident, such as an LLEA. This section should document the results of that planning.

This section should describe the response arrangements for security events, including their relationship with emergency situations and other contingency situations.

6.1 Response Plan and Arrangements

The section should describe the organizational onsite and offsite LLEA deployment arrangements, including an organizational chart or schematic that shows the management and organization structure and positions that interface with facility operations and security management and command and control responsibilities. It should provide a summary of the response force capabilities and deployment used for facility protection during a security event and other contingency situations (e.g., facility evacuation and fire). It should describe any compensatory measures that will be available during security events or other contingencies. It should identify how periodic testing, evaluation, and updating of the response plan and arrangements are undertaken.

6.2 Communications

If the LLEA is located on site, this section should describe the communication methods (e.g., radio and landlines) that response forces will use to communicate with the alarm monitoring station and to establish command and control during security events. It should include the following information:

- communication methods that will be used for all organizations providing response (e.g., onsite facility guards, the LLEA, and the military)

- an description of how these communication methods will be appropriately tested and maintained to ensure effective operability

- a schematic of the onsite response force communications network with available secure networks and linkages to the offsite LLEA or other organizations with which a support agreements exist

If the LLEA is off site, this section should describe the communication methods (e.g., landlines or radio) used to contact the LLEA to initiate a response.

6.3 Emergency Response and Contingency Planning

If the response force is located on site, this section should summarize the response force mission(s), capabilities, and deployment used for facility protection during security emergencies and other contingency situations (e.g., facility evacuation and fire). The plan should address emergency deployment of all response organizations. The plan should provide an organizational chart of the response force that shows the management and organization structure and key organizational interface positions with facility operations and security management. In addition, the section should provide a chart that shows the weapons and special equipment assigned to protective force personnel, including members of the initial armed response force. The plan should clearly establish which organization has overall command and control responsibility for facility emergencies and other contingency situations.

6.4 Increased Threat Level

This section should describe how notifications of an increased threat level are acted upon.

6.5 Security Event Reporting

This section should describe how security events are documented and reported to the facility security organization. The plan should describe how events are documented, who is responsible for documenting the event, and which subsequent reporting requirements are necessary (e.g., reporting to the NRC). The plan should also specify that the licensee should conduct a review of security arrangements after an event to evaluate the effectiveness of the facility security plan and procedures and to identify any improvements that may be necessary to optimize their effectiveness.

References

The licensee should list any reference documents, such as specific regulations, regulatory license, operating manuals, and organizational policies and manuals that are cited in the security plan or that are needed to explain or expand on any details in the plan.

Appendices

The licensee should provide or list the security implementing procedures, including their dates and version.

APPENDIX B

PHYSICAL SECURITY BEST PRACTICES FOR PANORAMIC AND UNDERWATER IRRADIATORS

Panoramic and underwater irradiators are generally used for commercial sterilization purposes. The two types of panoramic irradiators are dry source storage and wet source storage irradiators. The irradiator's radioactive sources are generally stored in a container constructed of solid material (e.g., concrete and lead) or in a water pool for shielding and then are brought out of the container/pool during normal operation to sterilize products located on stationary pallets or automated rack systems. Underwater irradiators remain in the water at all times; the product that will be irradiated is lowered into the pool. Panoramic and underwater irradiators are considered self-protecting during operation because the dose rate near the sources would cause incapacitation in a very short amount of time (e.g., seconds to minutes). Physical protection is generally needed to prevent the unauthorized removal of individual pencil sources when the irradiator is not in operation.

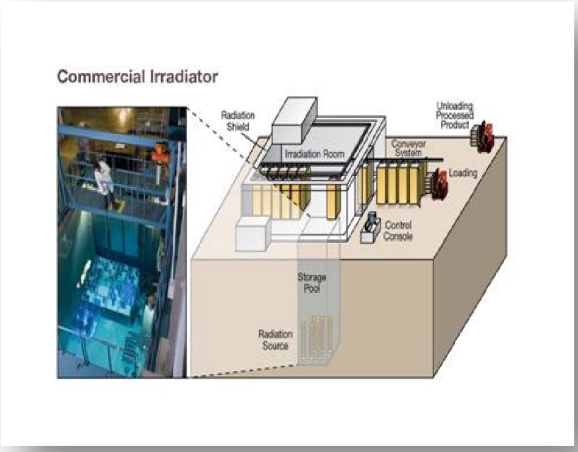

Figure B-1 Example of a commercial irradiator

B-1. Access Control

Generally, panoramic and underwater irradiator facilities are operational most of the time (e.g., 24 hours a day/7 days a week). Therefore, the access control measures must implement systems and procedures that only allow access into the security zone (e.g., irradiator control room and bunker/cell) by approved individuals (i.e., determined to be trustworthy and reliable). The licensee should consider the following access control measures for panoramic and underwater irradiator facilities:

- A continuous physical barrier should be used to limit access to the security zone. This zone will most likely be the control room and bunker/cell for these types of irradiators. The continuous barrier should have no openings other than access control points or material access openings that are large enough to allow a person to bypass the access control point and enter the security zone. For example, a wall should be continuous from the floor to the structural ceiling, and openings (such as vents) that are greater than 96 square inches, whereby the smallest dimension is greater than 6 inches, should have metal grates, bars, expanded metal (i.e., an industry term for a screen made of steel or a similarly strong metal through which an observer can see activities inside or outside an enclosure), or some other barrier that cannot be removed from outside the security zone.

- To help mitigate an insider threat, the licensee should consider installing an alarm or access control system, or both, that is separate (i.e., standalone) from the main facility security system in the security zone (e.g., irradiator control room and bunker/cell).

- Unescorted access to the security zone should be limited to only those individuals who require access to the irradiator or irradiator control room, or both, and who have been determined to be trustworthy and reliable based on NRC requirements.

- The security zone should use an access control system that has a minimum of two-factor identification, such as a key card and a personal identification number or biometric device. (See Section 3.1.5 of this NUREG report for more information.)

- If possible, the security zone should not include ancillary activities that do not specifically pertain to the storage and use of the irradiator (e.g., storage of irradiated product).

- Access control procedures should include a specific requirement to immediately deactivate or change access or alarm codes, or both, when an individual no longer requires unescorted access.

- Sites should install high-security locking systems and should remove exterior hardware from emergency exits and other doors if local health and safety rules or local fire building codes, or both, allow such measures. The locks should be specifically designed for security applications and should not be common builder's hardware-type locks found in home improvement stores.

- Keys used to operate the irradiator and to open the irradiator bunker/cell should be stored in a secured container when the irradiator is not in use.

- The licensee should control equipment used to move or handle sources because it can be used to facilitate access to, and removal of, the sources. Forklifts can be controlled by limiting key access or by not leaving the keys in the ignition. Likewise, other lifting mechanisms, such as cranes, can be controlled through the use of locks or other means.

Note that locks used for the irradiator bunker/cell door should allow for easy egress due to the high-radiation safety hazard.

B-2. Detection of Unauthorized Access

For the detection of unauthorized access into the security zone, the licensee should consider the following security measures:

- The licensee should form a sensor perimeter around the security zone by installing balanced magnetic switches (e.g., triple-biased switches) on the interior side of all applicable doors that cover all penetrations into the irradiator control room and entry and exit points for products.

- Security vendors can recommend the best types of alarm sensors; however, sensors should be of commercial quality similar to what a bank or another facility with high value assets would use. The licensee should avoid using typical home burglar alarm sensors.

- Security equipment rooms and telecommunications rooms that house security components, such as alarm control panels or uninterruptable power supplies (UPSs), should be secured, and access should only be granted to approved individuals who require access to these rooms.

- The licensee should use motion sensors that have at least two complementary technologies, such as passive infrared and microwave (e.g., dual technology motion detectors), to compensate for individual sensor technology limitations. Dual technology motion detectors can be programmed with the "AND" logic setting to require both sensors to detect an intruder before sending an alarm. This setting can cut down on nuisance alarms.

- Note that if the licensee installs the motion sensors or other electronic security equipment in the irradiator cell, the equipment must be able to withstand the high radiation levels in the room. Depending on the configuration of the facility or security zone, or both, the licensee should install sensors and security cameras in areas within the security zone (but outside of the irradiator cell) that can detect entry into the irradiator bunker/cell.

- Even if one sensor can provide adequate sensor coverage in a small room or space, a minimum of two sensors should still be built in as a compensatory measure. If one sensor becomes nonoperational, the remaining sensor can still provide alarm coverage for detection, thus saving the site from conducting compensatory measures until the sensor is operational again.

- The licensee should incorporate battery backup or UPS capability into the alarm systems. At least 2 hours of backup power should be available, and sites should have compensatory measure plans in place if power is not restored in the timeframe before the UPS is depleted.

- An offsite monitoring station or a protected onsite monitoring station, or both, should monitor alarms and video systems. If an offsite alarm monitoring station is used, it should be one that is approved by Underwriters Laboratories, Inc., and that can receive the alarms, assess the situation immediately, and dispatch the response force.

- An approved individual should be able to access covert and noncovert duress buttons to send a duress code/alarm from the irradiator control room (e.g., control panel) and the surrounding perimeter of the irradiator bunker.

- The licensee should also consider installing a radiation detection monitor to detect the removal of the radioactive source(s) from the irradiator bunker/cell. To mitigate the threat of an insider, the sensor should be separate from the security zone alarm system, should always be armed with no ability to disarm it, and should be able to send a separate signal/alarm to the monitoring station(s). The radiation detection monitors should be placed at the entry and exit points of the irradiator bunker/cell.

- Alarm systems should fail in an alarm condition if the power fails or if a signal wire is interrupted (e.g., a line cut).

- Use of supervised lines between the sensor and the alarm monitoring station and continuously monitored sensor tamper switches will help mitigate an insider threat.

- The licensee should periodically test, and perform maintenance on, alarms and associated systems.

B-3. Assessment of Alarms

The licensee should consider the following issues when assessing an alarm:

- The licensee must immediately assess instances of unauthorized access to ascertain the need for response.

- Video camera coverage (e.g., closed-circuit televisions (CCTVs), Internet protocol (IP) cameras, or captured video) of each sensor zone should provide assessment capability.

- The licensee should only use direct visual assessments for temporary purposes when, for example, the video assessment system is not functioning properly. For direct visual assessments, approved individuals should be properly trained on the process/procedures for assessing an alarm; this training should also include measures that approved individuals should take in the event of an armed or violent intrusion.

- Individuals should be easily recognizable when viewed on CCTV, IP cameras, or captured video. Achieving this level of resolution may necessitate the installation of appropriate lighting or cameras (e.g., cameras with infrared illumination) that can operate in low light conditions.

- The quality of the video system is a site decision that depends on the type of information that the licensee wants from the video images; however, a video system should have sufficient camera resolution to provide a clear picture to the monitoring station that shows unauthorized activity with the source device or sources. Higher quality video systems are readily available and may certainly be used if the site wants quality video images as evidence.

- The licensee should install cameras in vandal resistant enclosures, such as the typical “dome,” to prevent the accidental bumping or intentional tampering of the cameras.

- Alarm and video communication cables/lines should be able to detect tampering of the line (e.g., loss or interruption in signal) and should be physically protected inside conduit to the extent possible in accessible areas to prevent the easy cutting or manipulation of the cables/lines.

- Video should be recorded with the recorder located in a secure location. A digital video recorder (DVR) should be sufficient for most sites; however, larger sites may want to use network video recorders. The licensee should avoid using old video tape recorders because tapes degrade over time. Because some DVRs can be

programmed to record only when motion sensors detect motion, these recorders can easily store months of images.

- A method to differentiate between a duress alarm and other types of alarms (e.g., forced entry alarm) is beneficial when coordinating response activities.

B-4. Response

The licensee should consider the following factors when responding to an intrusion:

- Local law enforcement agencies (LLEAs) should have sufficient detailed information about the facility, descriptions of the radioactive sources or devices, and a description of the potential hazards associated with the sources to enable them to respond appropriately to any actual or attempted theft, sabotage, or diversion of the sources.

- The facility should have multiple ways to communicate (e.g., radios, landline telephones, and cell phones) to the response force (i.e., the LLEA). The licensee should locate communication devices at or near the control panel and irradiator bunker/cell.

- If the licensee uses a conventional radio system to communicate with the response force, it should assume that adversaries are eavesdropping on the transmission. The licensee should limit radio communications only to those transmissions that are absolutely necessary and that cannot be communicated by more secure methods, such as landline telephones and intercom systems. To help protect against deceptive messages, the licensee should use authentication codes to verify that the transmission was made by a member of the response force and not by an adversary.

- The licensee should conduct periodic testing of the alarm response with the LLEA.

- The licensee should coordinate with the LLEA at least annually or when changes to the facility design or operation adversely affect the potential vulnerability of the category 1 or category 2 quantities of radioactive material to theft, sabotage, or diversion.

APPENDIX C

PHYSICAL SECURITY BEST PRACTICES FOR SELF-SHIELDED IRRADIATORS

Self-shielded irradiators use radioactive sealed sources that are completely contained in a dry container constructed of solid materials (e.g., lead) and that are shielded at all times. As a result, they are inherently safe, and they can be stored in unshielded rooms. Self-shielded irradiators are typically located at hospitals, blood banks, universities, and research laboratories and are routinely used to irradiate research samples, small animals, and blood products.

Movable Source **Fixed (Nonmovable) Source** **Calibrator**

Figure C-1 Examples of self-shielded irradiators

C-1. Access Control

The licensee should consider the following access control measures for self-shielded irradiator facilities:

- A continuous physical barrier should be used to limit access to the security zone (i.e., the room in which the irradiator is located). The continuous barrier should have no openings other than access control points that are large enough to allow a person to bypass the access control point and enter the security zone. For example, a wall should be continuous from the floor to the structural ceiling, and openings (such as vents) that are greater than 96 square inches, whereby the smallest dimension is greater than 6 inches, should have metal grates, bars, expanded metal (an industry term for a screen made of steel or a similarly strong metal through which an observer can see activities inside or outside an enclosure), or some other barrier that cannot be removed from outside the security zone.

- Barrier walls should be of sound physical construction and should serve to delay an unauthorized intruder. Barrier boundaries that include windows (e.g., a glass window in a door) should not enable the direct viewing of the irradiator, and windows should be fixed and made of a robust glass (e.g., security glass with wire mesh to increase delay times).

- To help mitigate an insider threat, the licensee should consider installing an alarm or access control system, or both, that is separate (i.e., standalone) from the main facility security system in the security zone (e.g., irradiator room).

sufficient camera resolution to provide a clear picture to the monitoring station that shows unauthorized activity with the source device or sources. Higher quality video systems are readily available and may certainly be used if the site wants quality video images as evidence.

- The licensee should install cameras in vandal-resistant enclosures, such as the typical "dome," to prevent the accidental bumping or intentional tampering of the cameras.

- Alarm and video communication cables/lines should be able to detect tampering of the line (e.g., loss or interruption in signal) and should be physically protected inside conduit to the extent possible in accessible areas to prevent the easy cutting or manipulation of the cables/lines.

- Video should be recorded with the recorder located in a secure location. A digital video recorder (DVR) should be sufficient for most sites; however, larger sites may want to use network video recorders. The licensee should avoid using old video tape recorders because tapes degrade over time. Because some DVRs can be programmed to record only when motion sensors detect motion, these recorders can easily store months of images.

- A method to differentiate between a duress alarm and other types of alarms (e.g., forced entry alarm) is beneficial when coordinating response activities.

C-4 Response

The licensee should consider the following factors when responding to an intrusion:

- Local law enforcement agencies (LLEAs) should have sufficient detailed information about the facility, descriptions of the radioactive sources or devices, and a description of the potential hazards associated with the sources to enable them to respond appropriately to any actual or attempted theft, sabotage, or diversion of the sources.

- The facility should have multiple ways to communicate (e.g., radios, landline telephones, and cell phones) to the response force (i.e., the LLEA).

- If the licensee uses a conventional radio system to communicate with the response force, it should assume that adversaries are eavesdropping on the transmission. The licensee should limit radio communications only to those transmissions that are absolutely necessary and that cannot be communicated by more secure methods, such as landline telephones and intercom systems. To help protect against deceptive messages, the licensee should use authentication codes to verify that the transmission was made by a member of the response force and not by an adversary.

- The licensee should conduct periodic testing of the alarm response with the LLEA.

- The licensee should coordinate with the LLEA at least annually or when changes to the facility design or operation adversely affect the potential vulnerability of the category 1 or category 2 quantities of radioactive material to theft, sabotage, or diversion.

- Unescorted access to the security zone should be limited to only those individuals who require access to the irradiator and who have been determined to be trustworthy and reliable based on NRC requirements.

- Because keys and key cards can be lost or stolen, the security zone should use an access control system that has a minimum of two-factor identification, such as a key card and a personal identification number (PIN) or biometric device. (See Section 3.1.5 of this NUREG report for more information.)

- If possible, the security zone should not include ancillary activities that do not specifically pertain to the storage or use of the irradiator (e.g., research not related to irradiator use).

- Sites should install high-security locking systems and should remove exterior hardware from emergency exits and other doors if local health and safety rules or local fire building codes, or both, allow such measures. The locks should be specifically designed for security applications and should not be common builder's hardware-type locks found in home improvement stores.

- Keys used to operate the irradiator should be stored in a secured container when the irradiator is not in use.

- The access control or alarm system, or both, should also have the ability to send out a duress notification. The duress capability can be built into the access control readers or alarm panel. For example, a user may have his or her normal access PIN/code; however, he or she may also have a duress pin that will open the door and will covertly send a duress message to the monitoring station.

- The licensee should instruct and periodically test approved individuals (i.e., deemed to be trustworthy and reliable) who are assigned as escorts on access control procedures, including their specific responsibilities and expectations regarding access control. Note that multiple examples have occurred, whereby individuals who were responsible for maintaining access controls did not perform as expected because they were not fully trained on access control procedures. The training should include examples of scenarios that approved individuals could encounter (e.g., what to do when a colleague or maintenance personnel who does not have unescorted access authorization requires access to the irradiator room).

- Access control procedures should include a specific requirement to deactivate or change access or alarm codes, or both, when an individual no longer requires unescorted access.

- Individuals who have not been granted unescorted access authorization should be easily recognizable to individuals with unescorted access authorization (e.g., through the use of colored or special badges).

- To avoid bringing attention to the location of an irradiator, the licensee may decide not to place a "Caution Radioactive Materials" posting on the door to the irradiator room. Note that Title 10 of the *Code of Federal Regulations* (10 CFR) 20.1903, "Exceptions to Posting Requirements," allows an exception to radiological posting requirements, whereby the licensee is not required to post a caution sign in a room or area due to the presence of a

sealed source as long as radiation levels do not exceed 5 millirem per hour at 30 centimeters from source container. However, the licensee can reasonably post a caution sign on the device or in the immediate area.

- The license should control equipment used to move or handle sources because it can be used to facilitate access to, and removal of, the sources. Forklifts can be controlled by limiting key access or by not leaving the keys in the ignition. Likewise, other lifting mechanisms, such as cranes, can be controlled through the use of locks or other means.

C-2. Detection of Unauthorized Access

The licensee should consider the following security measures to detect unauthorized access into the security zone:

- All access points into the security zone should have the ability to detect, without delay, all unauthorized entries into the area. The licensee should use multiple methods to detect unauthorized access (e.g., a combination of balanced magnetic switch(s) on the access door(s) and motion detectors inside irradiator room).

- The licensee should only use direct control and constant surveillance for temporary or contingency purposes (e.g., if the irradiator or detection system is currently inoperable.)

- The licensee should use motion sensors that have at least two complementary technologies, such as passive infrared and microwave (e.g., dual technology motion detectors) to compensate for individual sensor technology limitations. Dual technology motion detectors can be programmed with the “AND” logic setting to require both sensors to detect an intruder before sending an alarm. This setting can cut down on nuisance alarms.

- Security vendors can recommend the best types of alarm sensors; however, sensors should be of commercial quality similar to what a bank or another facility with high value assets would use. The licensee should avoid using typical home burglar alarm sensors.

- The licensee should incorporate battery backup or uninterruptible power supply (UPS) capability into the alarm systems. At least 2 hours of backup power should be available, and sites should have compensatory measure plans in place if power is not restored in the timeframe before the UPS is depleted.

- Even if one sensor can provide adequate sensor coverage in a small room or space, a minimum of two sensors should be built in as a compensatory measure. If one sensor becomes nonoperational, the remaining sensor can still provide alarm coverage for detection, thus saving the site from conducting compensatory measures until the sensor is operational again.

- Consideration should be given for the use of irradiator room door closure alarms that generate an alarm signal if the door is not closed in a predetermined time period. Such alarms would identify situations in which the door has been propped open or has failed to fully close.

- An offsite monitoring station or a protected onsite monitoring station, or both, should monitor alarms and video systems. If an offsite alarm monitoring station is used, it should be one that is approved by Underwriters Laboratories, Inc., and that can receive the alarms, assess the situation immediately, and dispatch the response force.

- The licensee should also consider installing a radiation detection monitor and device tamper alarm to detect the removal of the radioactive source(s) from the irradiator room. To mitigate the threat of an insider, these sensors should be separate from the security zone alarm system, should always be armed with no ability to disarm them, and should be able to send a separate signal/alarm to the monitoring station(s).

- Security zone alarms should include both visible and audible alarm signals.

- Alarm systems should fail in an alarm condition if the power fails or if a signal wire is interrupted (e.g., a line cut).

- Use of supervised lines between the sensor and the alarm monitoring station and continuously monitored sensor tamper switches will help mitigate an insider threat.

- Security equipment rooms and telecommunications rooms that house security components, such as alarm control panels or the UPS, should be secured, and access should only be granted to approved individuals who require access to these rooms.

- The licensee should periodically test, and perform maintenance on, alarms and associated systems.

C-3. Assessment of Alarms

The licensee should consider the following issues when assessing an alarm:

- The licensee should immediately assess instances of unauthorized access to ascertain the need for response.

- Video camera coverage (e.g., closed-circuit televisions (CCTVs), Internet protocol (IP) cameras, or captured video) of each sensor zone should provide assessment capability.

- The licensee should only use direct visual assessments for temporary purposes when, for example, the video assessment system is not functioning properly. For direct visual assessments, approved individuals should be properly trained on the process/procedures for assessing an alarm; this training should also include measures that approved individuals should take in the event of an armed or violent intrusion.

- Individuals should be easily recognizable when viewed on CCTVs, IP cameras, or captured video. Achieving this level of resolution may necessitate the installation of appropriate lighting or cameras (e.g., cameras with infrared illuminators) that can operate in low light conditions.

- The quality of the video system is a site decision that depends on the type of information that the licensee wants from the video images; however, a video system should have

APPENDIX D

PHYSICAL SECURITY BEST PRACTICES FOR FIXED GAUGES

Fixed gauges containing radioactive materials are used for measuring the thickness of paper, steel, films, or other products; the density of materials; the level of materials in vessels and tanks; and the volumetric flow rate of products in piping. Fixed gauges are usually bolted to piping, vessels, or other equipment. The use of fixed gauges presents unique challenges with respect to source security. The guidance presented below provides best practices for the physical protection of fixed gauges.

Figure D-1 Example of a fixed gauge

Before developing a physical protection plan, fixed gauge licensees need to consider whether the quantity of radioactive material in their possession equals or exceeds the category 2 quantity of radioactive materials in Table 1 of Appendix A, "Category 1 and Category 2 Radioactive Materials," to Title 10 of the *Code of Federal Regulations* (10 CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material."

If a licensee has any single source that equals or exceeds the category 2 value in Appendix A to 10 CFR Part 37, it should comply with the requirements in 10 CFR Part 37. If a licensee does not have any single source that equals or exceeds the category 2 value, it needs to examine its radioactive material inventory and to determine whether it has a sufficient amount of activity to constitute an aggregated category 1 or category 2 quantity of radioactive material. Licensees can perform this determination using the guidance and sum of fractions calculation (unity rule) in Appendix A to 10 CFR Part 37.

The licensee possesses two sources in its inventory, for example, cesium-137 with an activity of 0.555 terabecquerel (TBq) (15 curies) and cobalt-60 with an activity of 0.185 TBq (5 curies). The category 2 value in Appendix A to 10 CFR Part 37 for these two sources is as follows:

- cesium-137 with an activity of 1 TBq (27 curies)
- cobalt-60 with an activity of 0.3 TBq (8.1 curies)

Neither one of these sources by itself equals or exceeds the category 2 threshold. By using the sum of fractions calculation in Appendix A to 10 CFR Part 37 for evaluating combinations of multiple sources to determine whether a location meets or exceeds the threshold, this calculates to be 1.17. In this case, because the sum is equal to, or greater than, unity (1), it would be considered a category 2 quantity of radioactive material and would require compliance with the requirements in 10 CFR Part 37 if the sources are only protected by a single physical barrier.

However, if additional physical barriers are present within the facility that would prevent access to a quantity of radioactive material that equals or exceeds the category 2 limits, the fixed gauges would not be considered aggregated, and implementation of the requirements in 10 CFR Part 37 would not be necessary. Examples of physical barriers for fixed gauges may include locked enclosures, such as rooms, cages, and metal enclosures, that completely encase the gauge and are permanently attached to some other immovable object, such as large pipes, tanks, beams, or a solid floor or ceiling. Examples of nonpermanent physical barriers include robust cables or chains with locks and tamper-proof mounting bolts (such as bolts with one-way threading and custom-designed heads, bolts welded in place, or locks used to prevent the removal or disassembly of gauge mounting hardware). As with any system, a barrier is only as strong as its weakest component. Therefore, for a licensee to consider a physical barrier to be effective and to take credit for the barrier, it should ensure that an adversary cannot bypass or easily defeat the barrier using commonly available tools. Specialty tools for the removal and installation of tamper-proof bolts should be secured and only accessible to approved individuals. In addition, the licensee must implement the requirements in 10 CFR Part 37 if a physical barrier, which has been installed to isolate the remaining aggregated gauges from other gauges, is breached (e.g., during a source exchange or gauge removal), and the total aggregated quantity of radioactive material is equal to, or greater than, the category 2 limits in 10 CFR Part 37.

D-1. Access Control

The licensee should consider the following access control measures for fixed gauge facilities:

Figure D-2 Example of a physical barrier surrounding a fixed gauge

- A continuous physical barrier should be used to limit access to the security zone. The continuous barrier should have no openings other than access control points that are large enough to allow a person to enter the security zone and bypass the access control point. For example, a wall should be continuous from the floor to the structural ceiling, and openings (such as vents) that are greater than 96 square inches, whereby the smallest dimension is greater than 6 inches, should have metal grates, bars, expanded metal (i.e., an industry term for a screen made of steel or a similarly strong metal through which an observer can see activities inside or outside an enclosure), or some other barrier that cannot be removed from outside the security zone.

- Unescorted access to fixed gauges that contain risk-significant radioactive material or an aggregated number of fixed gauges should be limited to individuals who are approved for access (i.e., determined to be trustworthy and reliable) and who require access to perform their job duties.

- The licensee should implement an access control system that is based on two modalities. For example, it should use electronic key card access for the fixed gauge areas and use a controlled physical key to access the individual rooms or buildings.

- Locks or chains, or both, used to secure radioactive sources should be specifically designed for security applications and should not be common builder's hardware-type locks found in home improvement stores. Keys for these locks should be secured and only accessible to authorized individuals.

- Specialty tools for the removal and installation of tamper-proof bolts should be secured and only accessible to approved individuals.

- The licensee should implement an access control system that uses a two-person protocol to access sources. This technique provides some mitigation for a lone insider performing a malevolent act. For this type of control system to be effective, no single individual would have access to both types of controls to gain access to the sources. For example, one individual would have electronic key card access, and the other individual would possess the physical key to locks.

- Because electronic key cards and physical keys are difficult to control, a better practice is to use electronic key cards in combination with something that is unique to the individual, such as a personal identification number code or biometric reader. This method is an example of two-factor identification. (See Section 3.1.5 of this NUREG report for more information.)

- Some electronic access control systems can be personalized to help prevent instances of unauthorized entry. For example, the licensee can limit access to a specific time period (e.g., access only granted from 6 a.m. to 6 p.m. (day shift) for an approved individual).

- Access control procedures should require locks, key cards, alarm codes, and passwords to be changed or deactivated immediately following personnel changes (e.g., employee termination).

- Equipment used to move or handle sources should be controlled because it can be used to facilitate access to, and the removal of, the sources. Forklifts can be controlled by limiting key access or by not leaving the keys in the ignition. Likewise, other lifting mechanisms, such as cranes, can be controlled through the use of locks or other means.

D-2. Detection of Unauthorized Access

For the detection of unauthorized access, licensee should consider the following:

- When rooms or buildings that house category 1 or category 2 quantities of fixed gauges are not under the control and constant surveillance by approved individuals, all access points to the fixed gauges should have the ability to detect,

without delay, all unauthorized entries into the area, including personnel access doors, gates, windows, vehicle rollup doors, and skylights. For example, a balanced magnetic switch on a personnel access door will be ineffective for detecting unauthorized access if the vehicle rollup door into the same area had no sensor and if the facility has no motion detectors in the area.

- Using more than one sensor to detect unauthorized access is preferable. The licensee should use sensors with different technologies when it incorporates two or more sensors into an area (e.g., the use of a balanced magnetic switch on the door into the area coupled with one or more dual-mode motion sensors (i.e., infrared (IR) and microwave sensors) inside of the area). The use of multiple technologies helps eliminate interference that might cause false alarms and makes an adversary's attempt to defeat detection more difficult.

- Keypads to the alarm system and communications panels should be located inside the protected area. Alarm systems generally have a delay feature that gives the licensee time to turn off the alarm system once the door is opened before it sends an alarm signal to the monitoring station.

- The licensee should incorporate battery backup or uninterruptible power (UPS) capability into the alarm systems. At least 2 hours of backup power should be available, and sites should have compensatory measures in place if power is not restored in the timeframe before the UPS is depleted.

- An offsite monitoring station or a protected onsite monitoring station should monitor alarms and video systems. If the licensee uses an offsite alarm monitoring station, it should be one that is approved by Underwriters Laboratories, Inc., and that can receive the alarms, assess the situation immediately, and dispatch the response force.

- Security zone alarms should include both visible and audible alarm signals.

- Alarm systems should fail in an alarm condition if the power fails or if a signal wire is interrupted (e.g., a line cut).

- The licensee should also consider using duress alarms (e.g., duress codes for alarm control panel or access control panel) for the fixed gauge area.

- The licensee should periodically test, and perform maintenance on, alarms and associate systems.

D-3. Assessment of Alarms

The licensee should consider the following issues when assessing an alarm for the areas with fixed gauges:

- The licensee should immediately assess instances of unauthorized access to ascertain the need for response.

- If approved individuals are used to assess an alarm, they should be well trained on what to do in the event of a malevolent act (e.g., get away from the area, hit the duress button, and call for help).

- Individuals should be easily recognizable when viewed on closed-circuit televisions (CCTVs), Internet protocol cameras, or captured video. Achieving this level of resolution may necessitate the installation of appropriate lighting or cameras that can operate in low light conditions (e.g., CCTV cameras equipped with IR illumination).

- The quality of the video system is a site decision that depends on the type of information that the licensee wants from the video images; however, a video system should have sufficient camera resolution to provide a clear picture to the monitoring station that shows unauthorized activity with the source device or sources. Higher quality video systems are readily available and may certainly be used if the site wants quality video images as evidence.

- The licensee should install cameras in vandal-resistant enclosures, such as the typical "dome," to prevent the accidental bumping or intentional tampering of the cameras.

- Alarm and video communication cables/lines should be able to detect tampering of the line (e.g., loss or interruption in signal) and should be physically protected inside conduit to the extent possible in accessible areas to prevent the easy cutting or manipulation of the cables/lines.

- Video should be recorded with the recorder located in a secure location. A digital video recorder (DVR) should be sufficient for most sites; however, larger sites may want to use network video recorders. The licensee should avoid using the old video tape recorders because tapes degrade over time. Because some DVRs can be programmed to record only when motion sensors detect motion, these recorders can easily store months of images.

- A method to differentiate between a duress alarm and other types of alarms (e.g., forced entry alarm) is beneficial when coordinating response activities.

- Fixed gauges are generally used for monitoring levels or flows in a process; therefore, when the process computers detect a failure in the gauge signal, the licensee should immediately evaluate the issue to ensure that a component has failed and that the failure is not due to an actual unauthorized access with an attempt to remove the gauge or the source from the gauge.

D-4. Response

The licensee should consider the following factors when responding to an unauthorized access:

- Onsite security personnel (if used) and local law enforcement agencies (LLEAs)

should have sufficient detailed information about the facility, descriptions of the radioactive sources or devices, and a description of the potential hazards associated with the sources to enable them to respond safely and effectively.

- The facility should have multiple ways to communicate (e.g., radios, landline telephones, and cell phones) to the response force (i.e., the LLEA). The licensee should locate communication devices in various areas within the facility.

- If the licensee uses a conventional radio system to communicate with the response force, it should assume that adversaries are eavesdropping on the transmission. The licensee should limit radio communications to only those transmissions that are absolutely necessary and that cannot be communicated by more secure methods, such as landline telephones and intercom systems. To help protect against deceptive messages, the licensee should use authentication codes to verify that the transmission was made by a member of the response force and not by an adversary.

- The licensee should conduct periodic testing of the alarm response with the LLEA.

- The licensee should coordinate with the LLEA at least annually or when changes to the facility design or operation adversely affect the potential vulnerability of the category 1 or category 2 quantities of radioactive material to theft, sabotage, or diversion.

APPENDIX E

PHYSICAL SECURITY BEST PRACTICES FOR MEDICAL DEVICES THAT CONTAIN RISK-SIGNIFICANT RADIOACTIVE MATERIAL

Medical devices that contain risk-significant radioactive material are generally used for the purpose of killing cancerous tissue, reducing the size of a tumor, or reducing pain. A teletherapy device is an example of a medical device that uses an intense beam of radiation from a powerful radioactive source, which is external to the patient and is focused on the cancerous tissue. A gamma stereotactic radiosurgery device is an example of a teletherapy device (e.g., the Gamma Knife® shown in Figure E-1). The Gamma Knife® focuses radiation from numerous cobalt-60 sources to a specific location deep within brain tissue.

Figure E-1 The Gamma Knife® (Courtesy of Elekta)

E-1. Access Control

The licensee should consider the following access control measures for medical devices that contain risk-significant radioactive material:

- A continuous physical barrier should be used to limit access to the security zone. This zone will most likely be the control room and the treatment room. The continuous barrier should have no openings other than access control points that are large enough to allow a person to enter the security zone and bypass the access control point. For example, a wall should be continuous from the floor to the structural ceiling, and openings (such as vents) that are greater than 96 square inches, whereby the smallest dimension is greater than 6 inches, should have metal grates, bars, expanded metal (i.e., an industry term for a screen made of

  steel or a similarly strong metal through which an observer can see activities inside or outside an enclosure), or some other barrier that cannot be removed from outside the security zone.

- Barrier walls should be of sound physical construction and should serve to delay an unauthorized intruder. Barrier boundaries that include windows (e.g., glass window in a door or wall) should be fixed and made of a robust glass (e.g., security glass with wire mesh to increase delay times).

- The licensee should limit unescorted access to the security zone only to those individuals who require access to the device or control room, or both, and who have been determined to be trustworthy and reliable based on U.S. Nuclear Regulatory Commission requirements.

- To help mitigate an insider threat, the licensee should consider installing an alarm or access control system, or both, that is separate (i.e., standalone) from the main facility security system in the security zone.

- Because keys and key cards can be lost or stolen, the security zone should use an access control system that has a minimum of two-factor identification, such as a key card and a personal identification number (PIN) or biometric device. (See Section 3.1.5 of this NUREG report for more information.)

- Sites should install high-security locking systems and should remove exterior hardware from emergency exits and other doors if local health and safety rules and fire building codes allow for such measures. The locks should be specifically designed for security applications and should not be common builder's hardware-type locks found in home improvement stores.

- Access control procedures should include a specific requirement to deactivate or change access or alarm codes, or both, when an individual no longer requires unescorted access.

- Individuals who have not been granted unescorted access authorization should be easily recognizable to individuals with unescorted access authorization (e.g., through the use of colored or special badges).

E-2. Detection of Unauthorized Access

For detection of unauthorized access into the security zone during times when the zone is not under constant surveillance by approved individuals, the licensee should consider the following security measures:

- All access points into the security zone should have the ability to detect, without delay, all unauthorized entries into the area. Multiple methods should be used to detect unauthorized access (e.g., a combination of balanced magnetic switch(s) on the access door(s) and motion detectors inside the treatment room and control room).

- The licensee should use motion sensors that have at least two complementary technologies, such as passive infrared and microwave (e.g., dual technology motion detectors), to compensate for individual sensor technology limitations. Dual technology motion detectors can be programmed with the "AND" logic setting to require both sensors to detect an intruder before sending an alarm. This setting can cut down on nuisance alarms.

- The licensee should incorporate battery backup or uninterruptible power supply (UPS) capability into the alarm systems. At least 2 hours of backup power should be available, and sites should have compensatory measure plans in place if power is not restored in the timeframe before the UPS is depleted.

- Security vendors can recommend the best types of alarm sensors; however, sensors should be of commercial quality similar to what a bank or another facility with high value assets would use. The licensee should avoid using typical home burglar alarm sensors.

- Even if one sensor can provide adequate sensor coverage in a small room or space, a minimum of two sensors should be built in as a compensatory measure. If one sensor becomes nonoperational, the remaining sensor can still provide alarm coverage for detection, thus saving the site from conducting compensatory measures until the sensor is operational again.

- An offsite monitoring station or a protected onsite monitoring station, or both, should monitor alarms and video systems. If the licensee uses an offsite alarm monitoring station, it should be one that is approved by Underwriters Laboratories, Inc., and that can receive the alarms, assess the situation immediately, and dispatch the response force.

- The licensee should also consider installing a radiation detection monitor and device tamper alarm to detect the removal of the radioactive source(s) from the medical device. To mitigate the threat of an insider, these sensors should be separate from the security zone alarm system, should always be armed with no ability to disarm them, and should be able to send a separate signal/alarm to the monitoring station(s).

- Security zone alarms should include both visible and audible alarm signals.

- Alarm systems should fail in an alarm condition if the power fails or if a signal wire is interrupted (e.g., a line cut).

- Use of supervised lines between the sensor and the alarm monitoring station and continuously monitored sensor tamper switches will help mitigate an insider threat.

- Security equipment rooms and telecommunications rooms that house security components, such as alarm control panels or the UPS, should be secured, and access should only be granted to approved individuals who require access to these rooms.

- An approved individual should be able to access covert and noncovert duress buttons to send a duress code/alarm from the treatment room (e.g., control panel) and the surrounding perimeter. Duress codes may also be programmed into automated access control systems or alarm systems, or both, to provide a user under duress the capability to open the access door and to covertly send a duress alarm to a monitoring station. For example, a user may have his or her normal access PIN; however, he or she may also have a duress pin that will open the door and will covertly send a duress message to the monitoring station.

- Increased delay or “hardening” in critical areas of the medical device increases the amount of time needed to remove radioactive material from the device and provides law enforcement additional time to respond before the material can be accessed.

- Currently, all new Gamma Knife® units are sold with increased delay from the factory, as a the result of a collaborative effort between Elekta and the Global Threat Reduction Initiative (GTRI), which is sponsored by the U.S. Department of Energy’s National Nuclear Security Administration. (See Appendix I of this NUREG report for more information about the GTRI.) In addition, a field-installable delay kit is currently being designed for these units to increase delay for Gamma Knife® units already at customer sites. The kit will be available for sites that are voluntarily cooperating with the GTRI on security enhancements.

- The licensee should periodically test, and perform maintenance on, alarms and associated systems.

E-3. Assessment of Alarms

The licensee should consider the following when assessing an alarm:

- The licensee should immediately assess instances of unauthorized access to ascertain the need for response.

- Video camera coverage (e.g., closed-circuit televisions (CCTVs), Internet protocol (IP) cameras, or captured video) of each sensor zone should provide assessment capability.

- The licensee should only use direct visual assessments for temporary purposes when, for example, the video assessment system is not functioning properly. For direct visual assessments, approved individuals should be properly trained on the process/procedures for assessing an alarm; this training should also include measures that approved individuals should take in the event of an armed or violent intrusion.

- Assessment capabilities should view the entrance and exit pathways from the treatment room(s) and any common work area within the treatment suite. Placement and installation of cameras inside the treatment room need to be coordinated with the facility management to avoid issues with patient confidentiality or the Health Insurance Portability and Accountability Act, or both.

- The quality of the video system is a site decision that depends on the type of information that the licensee wants from the video images; however, a video system should have sufficient camera resolution to provide a clear picture to the monitoring station that shows unauthorized activity with the source device or sources. Higher quality video systems are readily available and may be used if the site wants quality video images as evidence for law enforcement purposes.

- Individuals should be easily recognizable when viewed on CCTVs, IP cameras, or captured video. Achieving this level of resolution may necessitate the installation of appropriate lighting or cameras (e.g., cameras with infrared illuminators) that can operate in low light conditions.

- The licensee should install cameras in vandal-resistant enclosures, such as the typical “dome,” to prevent the accidental bumping or intentional tampering of the cameras. Camera viewing angles are often “adjusted” by users.

- Alarm and video communication cables/lines should be able to detect tampering of the line (e.g., loss or interruption in signal) and should be physically protected inside conduit to the extent possible in accessible areas to prevent the easy cutting or manipulation of the cables/lines.

- Video should be recorded with the recorder located in a secure location. A digital video recorder (DVR) should be sufficient for most sites; however, larger sites may want to use network video recorders. The licensee should avoid using old video tape recorders because tapes degrade over time. Because some DVRs can be programmed to record only when motion sensors detect motion, these recorders can easily store months of images.

- A method to differentiate between a duress alarm and other types of alarms (e.g., forced entry alarm) is beneficial when coordinating response activities.

E-4. Response

The licensee should consider the following factors when responding to an intrusion:

- Local law enforcement agencies (LLEAs) should have sufficient detailed information about the facility, descriptions of the radioactive sources or devices, and a description of the potential hazards associated with the sources to enable them to respond appropriately to any actual or attempted theft, sabotage, or diversion of the sources.

- The facility should have multiple ways to communicate (e.g., radios, landline telephones, and cell phones) to the response force (i.e., the LLEA).

- If the licensee uses a conventional radio system to communicate with the response force, it should assume that adversaries are eavesdropping on the transmission. The licensee should limit radio communications only to those transmissions that are absolutely necessary and that cannot be communicated by more secure methods, such as landline telephones and intercom systems. To help protect against deceptive messages, the licensee should use authentication codes to verify that the transmission was made by a member of the response force and not by an adversary.

- The licensee should coordinate with the LLEA at least annually or when changes to the facility design or operation adversely affect the potential vulnerability of the category 1 or category 2 quantities of radioactive material to theft, sabotage, or diversion.

APPENDIX F

PHYSICAL SECURITY BEST PRACTICES FOR MANUFACTURING AND DISTRIBUTION FACILITIES

Manufacturing and distribution (M&D) facilities are authorized under a U.S. Nuclear Regulatory Commission (NRC) or Agreement State license either to manufacture and distribute licensed nuclear materials or to distribute licensed nuclear materials manufactured by other licensees in the form of sealed radioactive sources. These sealed sources are used in various medical and industrial applications, including gamma stereotactic radiosurgery, high dose rate remote afterloaders, well logging, self-shielded and pool-type irradiators, fixed and portable nuclear gauges, and industrial radiography.

Some of these licensees receive unsealed nuclear material from various distributors within or outside of the United States and encapsulate this material into a special form sealed source with the use of a hot cell and remote manipulators. Other licensees receive these sealed sources from authorized manufacturers and commercially distribute them to licensees authorized to possess and use them for their intended applications. The sources manufactured and distributed under specific licenses include those that contain iridium-192, cobalt-60, cesium-137, and americium-241.

Figure F-1 Example of a hot cell with remote manipulators

F-1. Access Control

The access control measures must implement systems and procedures that include a robust system for detection of unauthorized access during the hours that the facility is unmanned. The access controls should include provisions for the simultaneous establishment of multiple temporary security zones on a relatively daily basis. The licensee should consider the following access control measures for M&D facilities:

- The licensee should use a continuous physical barrier to limit access to the permanent security zone, which is usually the area in the M&D facility in which sealed sources are manufactured or stored, or both, until they are distributed. This continuous barrier should have no openings other than access control points that are large enough to allow a person to enter the permanent security zone and bypass the access control point. For example, a wall should be continuous from the floor to the structural ceiling, and openings (such as vents) that are greater than 96 square inches, whereby the smallest dimension is greater than 6 inches, should have metal grates, bars, expanded metal (i.e., an industry term for a screen made of steel or a similarly strong metal through which an observer can see activities inside or outside an enclosure), or some other barrier that cannot be removed from outside the permanent security zone.

- The licensee must establish temporary security zones when moving licensed material out of the permanent security zone. During the establishment of these temporary security zones, the licensee should use personnel who have been deemed trustworthy and reliable to isolate this licensed material from unauthorized access.

- Access to the security zones should be limited to only those individuals who require access to the licensed material and who have been determined to be trustworthy and reliable based on NRC requirements.

- Because temporary security zones are regularly established within M&D facilities, the licensee must have the ability to immediately identify persons who are not approved to enter the temporary security zone. For example, approved individuals (those who have been determined trustworthy and reliable) should have a different color identification badge (or other distinguishing features) from those contractors and other persons who have not been granted authorization for access.

- To help mitigate an insider threat, the licensee should consider installing an alarm or access control system, or both, that is separate (i.e., standalone) from the main facility security system in the security zone (e.g., irradiator room).

- The permanent security zone should use an access control system that has a minimum of two-factor identification, such as a key card and a personal identification number (PIN) or biometric device. (See Section 3.1.5 of this NUREG report for more information.)

- M&D facilities should install high-security locking systems and should remove exterior hardware from emergency exits and other external doors if local health and safety rules or local fire building codes, or both, allow such measures. Locks selected should be specifically designed for security applications and should not be common builder's hardware-type locks found in home improvement stores.

- The access control or alarm system, or both, should also have the ability to send out a duress notification. The duress capability can be built into the access control readers or alarm panel. For example, a user may have his or her normal access PIN/code; however, he or she may also have a duress pin that will open the door and will covertly send a duress message to the monitoring station.

- Access control procedures should include a specific requirement to deactivate or change access or alarm codes, or both, when an individual no longer requires unescorted access.

- The licensee should control equipment used to move or handle sources because it can be used to facilitate access to, and removal of, the sources. Forklifts can be controlled by limiting key access or by not leaving the keys in the ignition. Likewise, other lifting mechanisms, such as cranes, can be controlled through the use of locks or other means.

F-2. Detection of Unauthorized Access

For the detection of unauthorized access into the permanent security zone, the licensee should consider the following security measures:

- All access points into the permanent security zone should have the ability to detect, without delay, all unauthorized entries into the area. Multiple methods should be used

to detect unauthorized access (e.g., a combination of balanced magnetic switch(s) on the access door(s) and motion detectors inside M&D room(s)).

- The licensee should use motion sensors that have at least two complementary technologies, such as passive infrared and microwave (e.g., dual technology motion detectors), to compensate for individual sensor technology limitations. Dual technology motion detectors can be programmed with the "AND" logic setting to require both sensors to detect an intruder before sending an alarm. This setting can cut down on nuisance alarms.

- Security vendors can recommend the best types of alarm sensors; however, sensors should be of commercial quality similar to what a bank or other facility with high value assets would use. The licensee should avoid using typical home burglar alarm sensors.

- Security equipment rooms and telecommunications rooms that house security components, such as alarm control panels or the UPS, should be secured, and access should only be granted to approved individuals (i.e., deemed to be trustworthy and reliable) who require access to these rooms.

- Even if one sensor can provide adequate sensor coverage in a small room or space, a minimum of two sensors should be built in as a compensatory measure. If one sensor becomes nonoperational, the remaining sensor can still provide alarm coverage for detection, thus preventing the M&D facility from conducting compensatory measures until the sensor is operational again.

- The licensee should incorporate battery backup or UPS capability into the alarm systems. At least 2 hours of backup power should be available, and sites should have compensatory measure plans in place if power is not restored in the timeframe before the UPS is depleted.

- An offsite monitoring station or a protected onsite monitoring station should monitor alarms and video systems. If the licensee uses an offsite alarm, it should be one that is approve by Underwriters Laboratories, Inc., and that can receive the alarms, assess the situation immediately, and dispatch the response force.

- The licensee should consider installing a radiation detection sensor to detect the removal of the radioactive sealed sources (or any unsealed licensed material) from the security zone. To mitigate the threat of an insider, the sensor should be separate from the security zone alarm system, should always be armed with no ability to disarm them, and should be able to send a separate signal/alarm to the monitoring station(s). The radiation detection monitors function as a redundant security feature. These monitors identify when licensed material is removed from the security zone because category 1 or category 2 quantities of radioactive material should never be stored during nonworking hours outside of the security zone.

- Security zone alarms should include both visible and audible alarm signals.

- Alarm systems should fail in an alarm condition if the power fails or if a signal wire is interrupted (e.g., a line cut).

- Security equipment rooms and telecommunications rooms that house security components, such as alarm control panels or the UPS, should be secured, and access should only be granted to approved individuals who require access to these rooms.

- Use of supervised lines between the sensor and the alarm monitoring station and continuously monitored sensor tamper switches will help mitigate an insider threat.

- The licensee should periodic test, and perform maintenance on, alarms and associated systems.

F-3. Assessment of Alarms

The licensee should consider the following when assessing an alarm:

- The licensee should immediately assess instances of unauthorized access to ascertain the need for response.

- Video camera coverage (e.g., closed-circuit televisions (CCTVs), Internet protocol (IP) cameras, or captured video) of each sensor zone should provide assessment capability.

- The licensee should only use direct visual assessments for temporary purposes when, for example, the video assessment system is not functioning properly. For direct visual assessments, approved individuals should be properly trained on the process/procedures for assessing an alarm; this training should also include measures that approved individuals should take in the event of an armed or violent intrusion.

- Individuals should be easily recognizable when viewed on closed-circuit televisions (CCTVs), Internet protocol cameras, or captured video. Achieving this level of resolution may necessitate the installation of appropriate lighting or cameras that can operate in low light conditions (e.g., CCTV cameras equipped with infrared illumination).

- The quality of the video system is a site decision that depends on the type of information that the licensee wants from the video images; however, a video system should have sufficient camera resolution to provide a clear picture to the monitoring station that shows unauthorized activity within the security zone(s) or to the facility surrounding the security zone(s). Higher quality video systems are readily available and may certainly be used if the site wants quality video images as evidence.

- The licensee should install cameras in vandal-resistant enclosures, such as the typical “dome,” to prevent the accidental bumping or intentional tampering of the cameras.

- Alarm and video communication cables/lines should be able to detect tampering of the line (e.g., loss or interruption in signal) and should be physically protected inside of conduit to the extent possible in accessible areas to prevent cutting or manipulation of the cables/lines.

- Video should be recorded with the recorder located in a secure location. A digital video recorder (DVR) should be sufficient for most sites; however, larger sites may want to use network video recorders. The licensee should avoid using old video tape recorders because tapes degrade over time. Because some DVRs can be programmed to record only when motion sensors detect motion, these recorders can easily store months of images.

- A method to differentiate between a duress alarm and other types of alarms (e.g., forced entry alarm) is beneficial when coordinating response activities.

F-4. Response

The licensee should consider the following should when responding to an intrusion:

- Local law enforcement agencies (LLEAs) should have sufficient detailed information about the facility, descriptions of the radioactive sources or devices, and a description of the potential hazards associated with the sources to enable them to respond appropriately to any actual or attempted theft, sabotage, or diversion of the sources.

- The facility should have multiple ways to communicate (e.g., radios, landline telephones, and cell phones) to the response force (i.e., the LLEA). The licensee should locate communication devices in various areas within the facility.

- If the licensee uses a conventional radio system to communicate with the response force, it should assume that adversaries are eavesdropping on the transmission. The licensee should limit radio communications should only to those transmissions that are absolutely necessary and that cannot be communicated by more secure methods, such as landline telephones and intercom systems. To help protect against deceptive messages, the licensee should use authentication codes to verify that the transmission was made by a member of the response force and not by an adversary.

- The licensee should conduct periodic testing of the alarm response with the LLEA.

- The licensee should coordinate with the LLEA at least annually or when changes to the facility design or operation adversely affect the potential vulnerability of the category 1 or category 2 quantities of radioactive material to theft, sabotage, or diversion.

APPENDIX G

PHYSICAL SECURITY BEST PRACTICES FOR WELL LOGGING SOURCES

Well logging that uses radioactive materials involves lowering a logging tool that contains a sealed radioactive source into a borehole to obtain and record information about the properties of the geologic formation and any fluids (e.g., oil, gas, and water) contained in the formation. Well logging operations generally involve the storage of radioactive sources at a field station or base camp, and then transporting and using them at the well site or drill site. Each of these activities presents unique challenges with respect to source security. The guidance presented below provides best practices for the physical protection of well logging activities.

Figure G-1 Well logging source transport containers

Before developing a physical protection plan, well logging licensees need to consider whether the quantities of radioactive material in their possession constitute an aggregated category 1 or category 2 quantity of radioactive material. If a licensee has any single source that equals or exceeds the category 2 value, it must comply with the requirements in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material." If a licensee does not have any single source that equals or exceeds the category 2 value in Appendix A to 10 CFR Part 37, it needs to examine its radioactive material inventory and to determine whether it has a sufficient aggregate amount of activity (i.e., material accessible by the breach of a single barrier) to constitute a quantity of concern. The licensee can perform this determination using the guidance and sum of fractions calculation (unity rule) in Appendix A, "Category 1 and Category 2 Radioactive Materials," to 10 CFR Part 37.

For example, if the licensee possesses two sources in its inventory as follows:

- cesium-137, with an activity of 0.250 terabecquerel (TBq) (6.76 curies) and americium-241/beryllium with an activity of 0.555 TBq (15 curies).

The category 2 value in Appendix A to 10 CFR Part 37 for these two sources is as follows:

- cesium-137 with an activity of 1 TBq (27 curies)
- americium-241/beryllium with an activity of 0.6 TBq (16.2 curies)

Neither one of these sources by itself equals or exceeds the category 2 threshold. By using the sum of fractions calculation in Appendix A to 10 CFR Part 37 for evaluating combinations of multiple sources to determine whether a location meets or exceeds the threshold, this calculates to be 1.1, which is greater than unity (1). The total amount would constitute a quantity of concern and would require compliance with the requirements in 10 CFR Part 37 if the sources are only protected by a single physical barrier.

G-1. SOURCE STORAGE AT A FIELD STATION OR BASE CAMP

G-1.1 Access Control

The licensee should consider the following access control measures for a well logging field station or base camp, or both:

- A continuous physical barrier should be used to limit access to the security zone. The continuous barrier should have no openings other than access control points that are large enough to allow a person to enter the security zone and bypass the access control point. For example, a wall should be continuous from the floor to the structural ceiling, and openings (such as vents) that are greater than 96 square inches, whereby the smallest dimension is greater than 6 inches, should have metal grates, bars, expanded metal (i.e., an industry term for a screen made of steel or a similarly strong metal through which an observer can see activities inside or outside an enclosure), or some other barrier that cannot be removed from outside the security zone.

- Unescorted access to source storage areas should be controlled and should be limited to only those individuals who have been approved for access (i.e., determined to be trustworthy and reliable) and who require access to perform their job duties.

- Locks, chains, and robust hardware used to secure radioactive sources should be specifically designed for high-security applications.

- The licensee should establish and implement an access control system that uses a two-person protocol to access sources. For this type of control system to be effective, no single individual would have access to both types of controls to gain access to the sources. For example, one individual would have electronic key card access, and the other individual would possess the physical key to the source storage pits.

- Because electronic key cards and physical keys can be difficult to control, a better practice is to use electronic key cards in combination with something that is unique to the individual, such as a personal identification number code or biometric reader. This method is an example of two-factor identification. (See Section 3.1.5 of this NUREG report for more information.)

- Some electronic access control systems can be personalized to prevent instances of unauthorized entry. For example, access can be limited to a specific time period (e.g., access only granted from 6 a.m. to 6 p.m.) for approved individuals.

- Access control procedures should require locks, key cards, and alarm code passwords to be updated or deactivated immediately following personnel changes (e.g., transfer, removal of duty, or termination of employees).

- The licensee should control equipment used to move or handle sources because it can be used to facilitate access to, and removal of, the sources. For example, forklifts that are used to move large transportation shields or lift covers off down-hole storage areas can be controlled by limiting key access or by not leaving the keys in the ignition. Likewise, other lifting mechanisms, such as cranes, can be controlled through the use of

locks or other means. Source handling tools and empty transportation containers should also be controlled and, if possible, stored separately from the sources.

G-1.2 Detection of Unauthorized Access

For the detection of unauthorized access, the licensee should consider the following security measures:

- When the source storage area is not under the control and constant surveillance of approved individuals, all entry points into the storage area should have the ability to detect, without delay, all unauthorized entries into the area, including personnel access doors, gates, windows, vehicle rollup doors, and skylights. For example, to ensure immediate detection of unauthorized entry to a source storage area that has multiple entries (e.g., personnel access doors and a vehicle rollup door), the licensee should use individual door sensors in combination with motion detectors to cover the entire storage area.

- Using two or more sensors with different technologies to detect unauthorized entry is preferable (e.g., a balanced magnetic switch on the door into the storage area used in conjunction with one or more dual-mode motion sensors (e.g., infrared and microwave sensors) inside the storage area). The use of multiple technologies (e.g., dual technology sensors) helps eliminate interference that might cause false alarms and makes an adversary's attempt to defeat detection more difficult.

- Keypads to the alarm system and communications panels should be readily accessible and should be inside the security zone or in a secured location. Alarm systems generally have a delay feature that gives the licensee time to deactivate the system before it sends an alarm signal to the monitoring station.

- The licensee should incorporate battery backup or uninterruptible power capability into alarm systems. At least 2 hours of backup power should be available, and sites should have compensatory measures in place if power is not restored in the timeframe before the backup power is depleted.

- An offsite monitoring station or a protected onsite monitoring station should monitor alarms and video systems. If the licensee uses an offsite alarm monitoring station, it should be one that is approved by Underwriters Laboratories, Inc., and that can receive the alarms, assess the situation immediately, and dispatch the response force.

- The licensee should install a siren and strobe outside the physical space to annunciate designated alarms, such as the remote monitoring system, when appropriate for facility operations.

- Alarm systems should fail in an alarm condition if the power fails or if a signal wire is interrupted (e.g., a line cut).

- The licensee should use duress alarms (e.g., duress codes for the alarm control panel (i.e., keypad)) for the source storage area.

- The licensee should periodically test, and perform maintenance on, alarms and associated systems.

- The licensee should establish a maintenance and testing program to ensure that security alarms and systems function as designed.

G-1.3 Assessment of Alarms

The licensee should evaluate instances of unauthorized access to determine the need for response. It should consider the following issues when assessing an alarm:

- If approved individuals are used to assess an alarm, they should be well trained on what to do in the event of a malevolent act (e.g., leave the area, call for help, and hit the duress button).

- Individuals should be easily recognizable when viewed on closed-circuit televisions, Internet protocol cameras, or captured video. Achieving this level of resolution may necessitate the installation of appropriate lighting or cameras that can operate in low light conditions (e.g., day/night cameras equipped with infrared illumination).

- The licensee should use cameras with sufficient resolution to provide a clear picture to the monitoring station that shows unauthorized activity with the source device or sources. Higher quality video systems are readily available and may be used if the site wants quality video images as evidence.

- The licensee should install cameras in vandal-resistant enclosures, such as the typical "dome," to prevent the accidental bumping or intentional tampering of the cameras.

- Alarm and video communication cables/lines should be able to detect tampering of the line (e.g., loss or interruption in signal) and should be physically protected inside conduit to the extent possible in accessible areas to prevent the easy cutting or manipulation of the cables/lines.

- Video should be recorded with the recorder located in a secure location. A digital video recorder (DVR) should be sufficient for most sites; however, larger sites may want to use network video recorders. The licensee should avoid using old video tape recorders because tapes degrade over time. Because some DVRs can be programmed to record only when motion sensors detect motion, these recorders can easily store months of images.

- During an assessment of alarms, programs should allow differentiation between a duress alarm and other types of alarms (e.g., forced entry alarm) when coordinating response activities.

G-1.4 Response

The licensee should consider the following factors when responding to unauthorized access at a field station or base camp, or both:

- Onsite security personnel (if used) and local law enforcement agencies (LLEA) should have sufficient detailed information about the facility, descriptions of the radioactive sources or devices, and a description of the potential hazards associated with the sources to allow them to respond appropriately to any actual or attempted theft, sabotage, or diversion of the radioactive materials.

- The field station or base camp should have multiple ways to communicate (e.g., radios, landline telephones, and cell phones) to the response force (the LLEA).

- If the licensee uses a conventional radio system to communicate with the response force, it should assume that adversaries are eavesdropping on the transmission. The licensee should limit radio communications only to those transmissions that are absolutely necessary and that cannot be communicated by more secure methods, such as landline telephones and intercom systems. To help protect against deceptive messages, the licensee should use authentication codes to verify that the transmission was made by a member of the response force and not by an adversary.

- The licensee should conduct periodic testing of the alarm response with the LLEA.

- The licensee should coordinate with the LLEA at least annually or when changes to the facility design or operation adversely affect the potential vulnerability of the category 1 or category 2 quantities of radioactive material to theft, sabotage, or diversion.

Figure G-2 Examples of source down-hole storage

G-2. USE AND TRANSPORTATION OF WELL LOGGING SOURCES

G-2.1 Access Control

For access authorization and control for the use and transport of well logging sources that constitute an aggregated amount of radioactive material, the licensee should consider the following access control measures:

- When well logging sources are in use and during their transportation, approved individuals (e.g., well logging crew determined to be trustworthy and reliable) have the responsibility for controlling access to the well logging sources. Therefore, the licensee should ensure that security procedures for controlling access and securing the source(s) are in place and that approved individuals are properly trained.

- The licensee should restrict access to well logging sources and transport vehicles to individuals who are approved for access and who require access to perform their job duties.

- Unless health and safety requirements for a site prohibit the disabling of the vehicle, a method should be used to disable the vehicle or trailer when it is not under direct control and constant surveillance by the licensee. For example, if the well logging crew stops for a meal or spends the night in a hotel, the well logging rig should have a disabling mechanism. Such mechanisms could include a physical means, such as wheel locks, or an electronic means associated with ignition controls. Different types of disabling mechanisms, depending on their robustness, will allow for varying degrees of delay.

- Controlling radioactive sources on vehicles requires two independent physical controls. For example, the source should be stored in a locked transport shield that is permanently fixed or chained to the vehicle and enclosed in a locked compartment.

- To mitigate an insider threat, a two-person access protocol should be followed. One individual could have access to the storage compartment, and another individual could have access to the lock on the transport container.

- Locks and chains used to control access should be robust and specifically designed for high-security applications.

Figure G-3 Storage compartment with a permanently mounted transport shield

G-2.2 Detection of Unauthorized Access

For the detection of unauthorized access, licensee should consider the following:

- During the transportation of well logging sources and when the vehicle/source is not under the constant control and surveillance of an approved individual (e.g., a person who is able to see the vehicle at all times), a method should be available to monitor and detect unauthorized access. A vehicle alarm system is normally an acceptable method. However, vehicle alarms should provide a local audible alarm and should transmit a signal/message to the approved individual's pager and cell phone and to a monitoring station during detection of unauthorized access.

- Licensees should consider using vehicle or package tracking systems, or both, to ensure that the vehicle or source, or both, is going to and from its intended destination. Some tracking systems can implement an "electronic fence" along the course of the approved route to or from the jobsite and can provide notification of any diversions off the route.

G-2.3 Response

The licensee should consider the following factors when responding to unauthorized access involving the use or transport of well logging source(s):

- Well logging crews transporting sources should have access to at least two different means of communication (e.g., radio and cell phone) to summon a response, if necessary.

- Crews should be familiar with any jobsite-specific procedures for requesting a response. Some jobsites may have an onsite security presence that may be able to support a response or to help summon the LLEA, if necessary.

APPENDIX H

PHYSICAL SECURITY BEST PRACTICES FOR INDUSTRIAL RADIOGRAPHY SOURCES

Appendix H provides physical security best practices to licensees that possess and use category 1 and category 2 sources for industrial radiography. Industrial radiography refers to examination of the structure of materials by nondestructive methods using ionizing radiation to make radiographic images, as authorized under Title 10 of the *Code of Federal Regulations* (10 CFR) Part 34, "Licenses for Industrial Radiography and Radiation Safety Requirements for Industrial Radiographic Operations," or equivalent Agreement State regulations.

Figure H-1 Industrial radiography camera

The radionuclides most commonly used for radiography are cobalt-60 and iridium-192; however, other radionuclides (e.g., californium-252, ytterbium-169, and selenium-75) with unique radiological characteristics might also be used. The physical security best practices identified relate to material in storage and transit.

Before developing a physical protection plan, industrial radiography licensees need to consider whether the quantities of radioactive material in their possession constitute an aggregated category 1 or category 2 quantity of radioactive material. If a licensee has any single source that equals or exceeds the category 2 value, it must comply with the requirements in 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material." If a licensee does not have any single source that equals or exceeds the category 2 value, it needs to examine its radioactive material inventory and to determine whether it has a sufficient aggregate amount of activity (i.e., material accessible by the breach of a single barrier) to constitute a quantity of concern. The licensee can perform this determination using the guidance and sum of fractions calculation (unity rule) in Appendix A, "Category 1 and Category 2 Radioactive Materials," to 10 CFR Part 37.

For example, if the licensee possesses two sources in its inventory as follows:

- iridium-192 with an activity of 0.60 terabecquerel (TBq) (16 curies) and cobalt-60 with an activity of 0.10 TBq (2.7 curies).

The category 2 value in Appendix A to 10 CFR Part 37 for these two sources is as follows:

- irridium-192 with an activity of 0.8 TBq (22 curies)
- cobalt-60 with an activity of 0.3 TBq (8.1 curies)

Neither one of these sources by itself equals or exceeds the category 2 threshold. By using the sum of fractions calculation in Appendix A to 10 CFR Part 37 for evaluating combinations of multiple sources to determine whether a location meets or exceeds the threshold, this calculates to be 1.06, which is greater than unity (1). The total amount would constitute a quantity of concern and would require compliance with the requirements in 10 CFR Part 37 if the sources are collocated and protected by a single physical barrier.

H-1. SOURCE STORAGE AT LICENSED LOCATIONS

H-1.1 Access Control

The licensee should consider the following access control measures for industrial radiography sources maintained in storage:

- A continuous physical barrier should be used to limit access to the security zone. The continuous barrier should have no openings other than access control points that are large enough to allow a person to enter the security zone and bypass the access control point. For example, a wall should be continuous from the floor to the structural ceiling, and openings (such as vents) that are greater than 96 square inches, whereby the smallest dimension is greater than 6 inches, should have metal grates, bars, expanded metal (i.e., an industry term for a screen made of steel or a similarly strong metal through which an observer can see activities inside or outside an enclosure), or some other barrier that cannot be removed from outside the security zone.

- Unescorted access to source storage areas should be controlled and limited to individuals who have been approved for access (i.e., determined to be trustworthy and reliable) and who require access to perform their job duties.

- Locks, chains, and robust hardware used to secure radioactive sources should be specifically designed for high-security applications.

- The licensee should establish and implement an access control system that uses a two-person protocol to access sources. For this type of control system to be effective, no single individual would have access to both types of controls to gain access to the sources. For example, one individual would have electronic key card access to the storage area, and the other individual would possess the physical key to unlock the chain or cabinet that secures the radiography device.

- Some electronic access control systems can be personalized to prevent instances of unauthorized entry. For example, access can be limited to a specific time period (e.g., access only granted from 6 a.m. to 6 p.m.) for approved individuals.

- Access control procedures should require keys and locks, key cards, passwords, and codes to alarm systems to be updated or deactivated immediately following personnel changes (e.g., transfer, removal from duty, or termination of employees).

- The licensee should control equipment used to handle sources because it can be used to facilitate the removal of the sources. For example, source handling tools and empty transportation containers should be controlled and stored away from the sources.

H-1.2 Detection of Unauthorized Access

For the detection of unauthorized access, the licensee should consider the following security measures:

- When the source storage area is not under the control and constant surveillance of approved individuals, all entry points into the storage area should have the ability to detect, without delay, all unauthorized entries into the area. Consideration should be given to personnel access doors, gates, windows, vehicle rollup doors, and skylights. For example, to ensure immediate detection of unauthorized entry to a source storage area that has multiple entries (e.g., personnel access door and vehicle rollup door), the licensee should use individual door sensors in combination with motion detectors to cover the entire storage area.

- Using two or more sensors with different technologies to detect unauthorized entry is preferable (e.g., the use of a balanced magnetic switch on the door into the storage area coupled with one or more dual-mode motion sensors (e.g., infrared and microwave sensors) inside the storage area). The use of multiple technologies (e.g., dual technology sensors) helps eliminate interference that might cause false alarms and makes an adversary's attempt to defeat detection more difficult.

- Keypads to the alarm system and communications panels should be readily accessible and should be inside the security zone or in a secured location. Alarm systems generally have a delay feature that gives the licensee time to deactivate the system before it sends an alarm signal to the monitoring station.

- The licensee should incorporate battery backup or uninterruptible power capability into alarm systems. At least 2 hours of backup power should be available, and sites should have compensatory measures in place if power is not restored in the timeframe before the backup power is depleted.

- An offsite monitoring station or a protected onsite monitoring station should monitor alarms and video systems. If the licensee uses an offsite alarm monitoring station, it should be one that is approved by Underwriters Laboratories, Inc., and that can receive the alarms, assess the situation immediately, and dispatch the response force.

- Alarm systems should fail in an alarm condition if the power fails or if a signal wire is interrupted (e.g., a line cut).

- The licensee should use duress alarms (e.g., duress code for alarm control panel (i.e., keypad)) for the source storage area.

- The licensee should periodically test, and perform maintenance on, alarms and associated systems.

- The licensee should establish a maintenance and testing program to ensure that security alarms and systems function as designed.

H-1.3 Assessment of Alarms

The licensee should evaluate instances of unauthorized access to determine the need for response. It should consider the following issues when assessing an alarm for the source storage area:

- If approved individuals are used to assess an alarm, the individuals should be well trained on what to do in the event of a malevolent act (e.g., leave the area and call for help and hit the duress button).

- Individuals should be easily recognizable when viewed on closed-circuit televisions, Internet protocol cameras, or captured video. Achieving this level of resolution may necessitate the installation of appropriate lighting or cameras that can operate in low light conditions (e.g., day/night cameras equipped with infrared illumination).

- The licensee should use cameras with sufficient resolution to provide a clear picture to the monitoring station that shows unauthorized activity with the source device or sources.

- The licensee should install cameras in vandal-resistant enclosures, such as the typical “dome,” to prevent the accidental bumping or intentional tampering of the cameras.

- Alarm and video communication cables/lines should be able to detect line tampering (e.g., loss or interruption in signal) and should be physically protected inside conduit to the extent possible in accessible areas to prevent the easy cutting or manipulation of the cables/lines.

- Video should be recorded with the recorder located in a secure location. A digital video recorder (DVR) should be sufficient for most sites; however, larger sites may want to use network video recorders. The licensee should avoid using old video tape recorders because tapes degrade over time. Because some DVRs can be programmed to record only when motion sensors detect motion, these recorders can easily store months of images.

- During an assessment of alarms, programs should allow differentiation between a duress alarm and other types of alarms (e.g. forced entry alarm) when coordinating response activities.

H-1.4 Response

The licensee should consider the following factors when responding to unauthorized access at an industrial radiography source storage location:

- Onsite security personnel (if used) and local law enforcement agencies (LLEA) should have sufficient detailed information about the facility, descriptions of the radioactive sources or devices, and a description of the potential hazards associated with the sources to enable them to respond appropriately to any actual or attempted theft, sabotage, or diversion of the radioactive materials.

- The storage area should have multiple ways to communicate (e.g., radios, landline telephones, and cell phones) to the response force (the LLEA).

- If the licensee uses a conventional radio system to communicate with the response force, it should assume that adversaries are eavesdropping on the transmission. The licensee should limit radio communications only to those transmissions that are absolutely necessary and that cannot be communicated by more secure methods, such as landline telephones and intercom systems. To help protect against deceptive messages, the licensee should use authentication codes to verify that the transmission was made by a member of the response force and not by an adversary.

- The licensee should conduct periodic testing of the alarm response with the LLEA.

- The licensee should coordinate with the LLEA at least annually or when changes to the facility design or operation adversely affect the potential vulnerability of the category 1 or category 2 quantities of radioactive material to theft, sabotage, or diversion.

H-2. USE AND TRANSPORTATION OF INDUSTRIAL RADIOGRAPHY SOURCES

H-2.1 Access Control

The licensee should consider the following access control measures for the use and transport of industrial radiography sources:

- When in use and during transportation of industrial radiography sources, the approved individuals (i.e., radiographers determined to be trustworthy and reliable) have the responsibility for controlling access to the sources. Therefore, the licensee must ensure that security procedures for controlling access and securing the source(s) are in place and that approved individuals are properly trained.

- The licensee should restrict access to industrial radiography sources and transport vehicles to individuals who are approved for access and who require access to perform their job duties.

- Unless health and safety requirements for a site prohibit the disabling of the vehicle, a method should be used to disable the vehicle or transport trailer when it is not under direct control and constant surveillance by the licensee. For example, if the radiographer(s) stops for a meal or spends the night in a hotel, the transport vehicle should have a disabling mechanism. Such mechanisms could include a physical means, such as wheel locks, or an electronic means associated with ignition controls. Different types of disabling mechanisms, depending on their robustness, will allow for varying degrees of delay.

- Controlling radioactive sources on vehicles requires two independent physical controls. For example, the source should be stored in a locked transport shield that is permanently fixed or chained to the vehicle and enclosed in a locked compartment.

- Locks and chains used to control access should be robust and specifically designed for high-security applications.

H-2.2 Detection of Unauthorized Access

For the detection of unauthorized access, the licensee should consider the following security measures:

- During the transportation of industrial radiography sources and when the vehicle/source is not under the constant control and surveillance of an approved individual, a method should be available to monitor and detect unauthorized access. A vehicle alarm system should be used to satisfy the requirement. Vehicle alarms should provide a local audible alarm and should transmit a signal/message to the approved individual's pager and cell phone and to a monitoring station during detection of unauthorized access.

- Licensees should consider using vehicle or package tracking systems, or both, to ensure that the vehicle or source, or both, is going to and from its intended destination. Some tracking systems can implement an "electronic fence" along the course of the approved route to or from the jobsite and can provide notification of any diversions off the route.

Figure H-2 Secured radiography darkroom truck

H-2.3 Response

The licensee should consider the following when responding to unauthorized access involving the use or transport of industrial radiography sources:

- Radiography crews transporting sources should have access to at least two different means of communication (e.g., a radio and cell phone) to summon a response, if necessary.

- Radiographers should be familiar with any jobsite-specific procedures for requesting a response. Jobsites may have an onsite security presence that may be able to support the response or to help summon LLEA, if necessary.

APPENDIX I

GLOBAL THREAT REDUCTION INITIATIVE PROGRAM

The Global Threat Reduction Initiative (GTRI) is part of the U.S. Department of Energy's National Nuclear Security Administration (NNSA). With partners in more than 100 countries to include working domestically within the United States, the GTRI's mission is to reduce and protect vulnerable nuclear and radioactive material located at civilian sites worldwide.

The GTRI is a "first line of defense" program that works to prevent terrorists from acquiring materials that could be used in a weapon of mass destruction, a crude nuclear bomb, a radioactive dirty bomb, or other acts of terrorism. Participation with the NNSA's GTRI program by interested sites is voluntary, and all the security enhancements and training provided by the GTRI are federally funded.

I-1. Materials of Concern

Thousands of civilian sites use nuclear and radioactive materials for legitimate and beneficial commercial, medical, and research purposes. Materials of concern are found in soft targets, such as hospitals and universities, which are open environments that often lack armed onsite guards. A radiological dispersal device, deployed with amounts of radioactive material found in normal use at these types of facilities, could result in radioactive contamination that could require relocation, prohibit the use of that area pending decontamination, and potentially cause economic impacts in the billions of dollars.

I-2. Domestic Security Enhancement Program

In the United States, the GTRI further enhances the protection of nuclear and radioactive materials at civilian sites through voluntary security enhancement efforts. These efforts complement, but do not replace, U.S. Nuclear Regulatory Commission (NRC) and Agreement State requirements. They are federally funded, cost-effective, and prudent best practices that further improve security above regulatory requirements. These upgrades and best practices have been implemented at more than 1,500 sites that are cooperating with the GTRI worldwide.

These efforts include the activities:

- Removal. This activity involves the recovery of unwanted radioactive sources.
- Detection. This activity involves the installation of remote monitoring systems (RMSs), access control devices, intrusion detection systems, and video surveillance systems.
- Delay. This activity involves the deployment of in-device delay (IDD) mechanisms, tie downs, pool covers for panoramic irradiators, and hardened doors and rooms.
- Response. This activity involves training for first responders and table top exercises for sites and local response agencies.

I-3. Removal

Every year, NNSA's Off-Site Source Recovery Program removes thousands of sources that are disused and unwanted in the United States. To learn more and to register unwanted sealed sources visit Los Alamos National Laboratory's Web site at http://osrp.lanl.gov/.

I-4. Detection

Through the GTRI, NNSA offers voluntary security enhancements to prevent and detect unauthorized activity. Detection upgrades include the following:

- biometric access control devices
- intrusion detection systems (i.e., motion sensors and door alarms)
- Surveillance cameras
- radiation monitors
- electronic tamper-indicating seals
- RMSs

Through the GTRI, NNSA offers an RMS, which is critical for addressing the insider threat and for improving alarm communications and local law enforcement response. This best practice is in addition to the facility intrusion detection system and focuses on detection of insiders attempting unauthorized access to the radioactive or nuclear material. The RMS integrates insider protection measures (e.g., irradiator tampering to detect unauthorized access, radiation monitoring to detect a source outside its shielding, and communication/power loss for the detection system) with video images in a tamper-indicating housing with an uninterruptable power supply to ensure the RMS continues to function during a power loss. The RMS encrypts the video and alarm data and sends it simultaneously to onsite security and offsite local law enforcement or alarm stations to prevent single-point failures in alerting armed responders to a potential theft.

I-5. Delay

The GTRI provides delay enhancements that impede an adversary's ability to access nuclear materials and radioactive sources. By increasing delay, first responders have more time to interrupt the adversary before he or she can remove and then leave the facility with these materials. These delay systems include the following items:

- device tie downs and security cages
- security grating
- hardened doors and rooms
- ballistic glass
- alarmed pool covers for panoramic wet source storage irradiators
- IDD kits

In cooperation with NRC and the U.S. Department of Homeland Security (DHS), NNSA has collaborated with cesium irradiator manufacturers to develop IDD kits for the most widely used models of cesium chloride blood and research irradiators. The GTRI currently funds the installation of IDD kits for Best Theratronics Gammacell 40, 1000, and 3000; JL Shepherd Mark 1 and Model 143; and Pharmalucence (CIS) IBL-437C at volunteer facilities. IDD enhancements add a set of protection hardware, including hardened security plates and tamper-resistant fasteners to the irradiator, which greatly increases delay times without affecting normal operation, use, and maintenance. The IDD kit provides first responders with valuable extra time to respond and prevent material from leaving the facility.

I-6. Response

The GTRI provides site personnel and first responders with specialized tools and training to respond to a security incident at civilian sites with nuclear and radioactive materials. This response support includes the following items:

- enhanced radio systems and repeaters
- personal radiation detectors
- Central Alarm Station hardening
- RMS alarm review stations
- alarm response training
- table top exercises

I-7. Monitoring Centers

NNSA provides support to State, regional, and local organizations that are interested in monitoring the nuclear and high-activity radioactive materials within their boundaries. This enables first responders to have immediate situational awareness about an attempted attack at nuclear or radioactive material sites.

I-8. Alarm Response Training

The GTRI offers a three-day course that is held at the NNSA facility in Oak Ridge, TN. This training does the following:

- It teaches site-level operations and security staff and local law enforcement how to protect themselves and their communities when responding to alarms indicating possible theft of civilian nuclear and radioactive materials.
- It includes realistic scenarios using radioactive sources, irradiators, and the same type security equipment provided by the GTRI at participating sites.

- It provides classroom instruction and hands-on exercises.

The course is certified by DHS. Through the GTRI, NNSA pays for all attendee costs except for salary (e.g., travel, lodging, car rental, and per diem).

I-9. Table Top Exercises

NNSA and the Federal Bureau of Investigation (FBI) sponsor no-fault, site-specific scenarios that allow officials to exercise their response to terrorist acts involving nuclear and radioactive materials. The exercises do the following:

- Promote cross-sector communication, cooperation, and team building among Federal, State, local, and private sector first responders.

- Examine newly developed tactics, techniques, and procedures resulting from GTRI voluntary security enhancements.

- Offer a one-day exercises in near-real-time game play customized to the specific site with realistic events based on FBI threat information and video injections with mock-media involvement for fast-paced action.

I-10. Domestic Security Enhancements Summary

In summary, the GTRI offers the following elements as part of its Domestic Security Enhancement Program:

- a voluntary program for civilian sites with nuclear and radioactive materials and their first responders

- Federally funded security enhancements, including a minimum of 3 years of warranty and maintenance support

- assistance in nuclear and radioactive material removals, detection, delay, and response

- an alarm response training course at the NNSA facility in Oak Ridge, TN

- table top exercises that involve no-fault, site-specific scenarios

I-11. Additional Information

SECY-10-0036, “Update on Staff Efforts To Work with Federal Partners on Voluntary Security Initiatives for Radioactive Materials,” U.S. Nuclear Regulatory Commission, Washington, DC, March 30, 2010. (This policy issue information report is available on the NRC Web site at www.nrc.gov.)

Regulatory Information Summary 2010-02, “The Global Threat Reduction Initiative (GTRI) Federally Funded Voluntary Security Enhancements for High-Risk Radioactive Material,”

U.S. Nuclear Regulatory Commission, Washington, DC, January 21, 2010. (This report is available on the NRC Web site at www.nrc.gov.)

Interested in volunteering? Have greater than 10 curies of cesium-137, cobalt-60, americium-241, iridium-192, or any other isotope of concern (i.e., selenium-75, strontium-90, thulium-170, ytterbium-169, polonium-210, radium-226, plutonium-238, plutonium-239, curium-244, or californium-252)? Contact the GTRI at GTRIinfo@nnsa.doe.gov.

NRC FORM 335
(12-2010)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG-2166

2. TITLE AND SUBTITLE

Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material

3. DATE REPORT PUBLISHED

MONTH	YEAR
May	2014

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

A. Gaudreau, P. Goldberg, C. Gordon, S. Hawkins, J. Katanic, K. Lambert, W. Lee, F. Pavlechko, G. Purdy, R. Ragland, J. Thompson, A. True, D. White

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

May 2014 - May 2019

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Division of Material Safety and State Agreements
Office of Federal and State, Materials and Environmental Management Programs
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)

Same as above

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

This document provides guidance to Nuclear Regulatory Commission (NRC) licensees or applicants regarding developing and implementing a physical protection program for the protection of risk-significant radioactive materials (e.g., category 1 and category 2 quantity of radioactive materials). This information is intended to provide NRC licensees or applicants guidance with specific emphasis on physical security best practices. The approaches and methods in this document are not requirements but the NRC considers them to be acceptable for complying with the requirements in Title 10 of the Code of Federal Regulations (10 CFR) Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material."

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

NUREG
Part 37
Physical Protection
Best practices

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

(This Page)
unclassified

(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS

STAY CONNECTED

NUREG-2166

Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material

May 2014